firm

Kundenleitfaden

Grundsätzliches zur Sicherheit von PCs
Sicherheit innerhalb von SFirm erhöhen

Finanzen. Professionell. Managen.

Dezember 2024

Inhalt

Copyrights und Warenzeichen

Windows, Windows Server, SQL Server und Hyper-V sind eingetragene Warenzeichen der Microsoft Corp. Alle in dieser Dokumentation zusätzlich verwendeten Programmnamen und Bezeichnungen sind u.U. ebenfalls eingetragene Warenzeichen der Herstellerfirmen und dürfen nicht gewerblich oder in sonstiger Weise verwendet werden. Irrtümer vorbehalten.

Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt gearbeitet. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Die angegebenen Daten dienen lediglich der Produktbeschreibung und sind nicht als zugesicherte Eigenschaft im Rechtssinne zu verstehen.

Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder juristische Verantwortlichkeit noch irgendeine Haftung übernehmen. Alle Rechte vorbehalten; kein Teil dieser Dokumentation darf in irgendeiner Form (Druck, Fotokopie oder die Speicherung und/oder Verbreitung in elektronischer Form) ohne schriftliche Genehmigung der Star Finanz-Software Entwicklung und Vertriebs GmbH reproduziert oder vervielfältigt werden.

Die Star Finanz entwickelt ihre Produkte ständig weiter, um Ihnen den größtmöglichen Komfort zu bieten. Deshalb bitten wir um Verständnis dafür, dass sich Abweichungen vom Handbuch zum Produkt ergeben können.

Star Finanz-Software Entwicklung und Vertriebs GmbH - Grüner Deich 15 - 20097 Hamburg

1 Grundsätzliches zur Sicherheit eines PCs

1.1 Einführung

Banking und Finanzmanagement mit SFirm: da können Sie sich sicher sein!

Die Daten Ihrer Unternehmensfinanzen sind ein besonders sensibles Gut - von daher stehen Sicherheit und Datenschutz bei SFirm an erster Stelle. Damit Sie darauf bei Ihrem Banking und Finanzmanagement vertrauen können, verwendet SFirm vielfältige und ausgefeilte Schutzmechanismen. So sind Sie immer bestmöglich vor sich ständig verändernden Bedrohungen geschützt.

Nachfolgend führen wir einige Schutzmaßnahmen auf, mit denen Sie die Sicherheit bei der Nutzung von SFirm erhöhen können.

Welche Maßnahmen gibt es?

Neben den bereits in SFirm integrierten Schutzmechanismen gibt es auf der Systemseite mehrere wichtige und effektive Maßnahmen:

1.2 Windows-Updates

Ihr Windows Betriebssystem sollte immer auf dem aktuellen Stand gehalten werden. Microsoft verteilt dazu Updates, die standardmäßig automatisch installiert werden.

Ist Ihr PC Teil eines Netzwerkes, kann es sein, dass die Windows-Updates von Ihrem Systembetreuer verwaltet werden. Bei Problemen mit den Windows-Updates sollten Sie sich in diesem Fall an Ihren Systembetreuer wenden.

Um zu überprüfen, ob sich Ihre Windows-Updates auf dem neusten Stand befinden, können Sie über das Suchfeld in Windows die *Windows Update-Einstellungen* aufrufen.

1.3 Schutzsoftware

Generell sollte auf jedem PC eine Schutzsoftware (Virenscanner, Internet Security, etc.) installiert sein, um Ihre Daten vor Angriffen jeglicher Art, also aus dem Internet, über USB-Sticks oder auch E-Mails, zu schützen. Natürlich kann es keinen hundertprozentigen Schutz geben. Je aktueller allerdings Ihre Schutzsoftware gehalten wird, umso sicherer ist ihr PC.

Bitte setzen Sie eine Schutzsoftware ein.

1.4 Firewalls

Firewalls sind ein wichtiger Teil des Schutzkonzepts für PCs und Netzwerke. Sie regeln, zu welchen Adressen jemand eine Verbindung im Internet aufnehmen darf, aber auch von welchen Adressen eine Verbindung in Ihr Netzwerk aufgebaut werden darf.

Da SFirm eine Verbindung zu einem Bankrechner aufbauen möchte, ist es deshalb wichtig die Adresse des Bankrechners in der Firewall bekannt zu machen. Bei Netzwerken ist hierfür wieder der Systembetreuer zuständig.

SFirm nimmt nicht nur den Kontakt zum Bankrechner auf, sondern wird auch den Kontakt zu Adressen der Star Finanz suchen, z.B. um die Lizenz zu überprüfen oder um Updates für SFirm herunterzuladen.

Neben den Adressen der Bankrechner, die Ihnen in der Regel mit den Zugangsdaten mitgeteilt werden, wird SFirm versuchen folgende Adressen zu erreichen:

Freigeschaltete Adressen	• www.sfirm.de • download.sfirm.de • downloads.starfinanz.de (CDN, daher keine statische IP verfügbar) • services.starfinanz.de • finanzcockpit.starfinanz.de
Freigeschaltete Ports	• 53 (DNS Nameservice) • 80 (http) • 443 (https)

1.5 Aktive Festplattenverschlüsselung

Damit Ihre Finanzdaten bestmöglich geschützt sind, verwenden Sie bitte auf dem Datenträger, der die SFirm-Daten und Datenbanken (MS SQL Server) enthält, eine aktive Laufwerksverschlüsselung.

Bitte prüfen Sie, ob dies bereits der Fall ist. Wenn nicht, empfehlen wir Ihnen im Rahmen Ihrer Datensicherheit dringend, eine Festplattenverschlüsselung einzusetzen. Beispiel: BitLocker.

1.5.1 BitLocker

BitLocker ist eine Festplattenverschlüsselung von Microsoft. Sie ist verfügbar in:

- Windows 10
- Windows 11
- Ab Windows Server 2016

Weitere Informationen zu BitLocker bei Microsoft

1.6 Restriktive Zugriffsberechtigungen

Für einen optimalen Datenschutz ist es ebenso notwendig, dass die von SFirm verwendeten Installations- und Datenbankverzeichnisse mittels Zugriffsbeschränkungen (z.B. über Windows-Rechte) abgesichert sind. Bitte stellen Sie sicher, dass nicht jeder Nutzer, sondern nur die Nutzer, die die Software verwenden dürfen, die entsprechenden Zugriffsrechte besitzen.

Folgende SFirm-Verzeichnisse sollten unbedingt gegen den unberechtigten Zugriff geschützt werden, indem die Zugriffsrechte für andere Benutzer/-gruppen entzogen werden.

Beispiel lokale SFirm-Installation:

- SFirm-Programmverzeichnis, z.B. C:\Program Files (x86)\SFirmV4
- SFirm-Datenverzeichnis, z.B. C:\ProgramData\SFirmV4
- Weitere SFirm-Mandantenverzeichnisse (sofern vorhanden), z.B. C:\ProgramData\SFirmV4-Mandanten
- Datenbank-Pfad auf <RECHNERNAME>, z.B. C:\Program Files\SFirm SQL Server

Beispiel SFirm-Netzwerkinstallation:

- SFirm-Programmverzeichnis, z.B. C:\Program Files (x86)\SFirmV4
- SFirm-Datenverzeichnis, z.B. \\SERVER\FREIGABE1\SFirmV4
- Weitere SFirm-Mandantenverzeichnisse (sofern vorhanden), z.B. \\SERVER\FREIGABE1\SFirmV4-Mandanten
- Datenbank-Pfad auf dem MS SQL Server, z.B. C:\Programme\Microsoft SQL Server\

Damit Ihr System bestmöglich abgesichert ist, melden Sie sich bitte bei der täglichen Arbeit mit SFirm mit einem Windows-Benutzer an Ihrem Computer an.

Sind Sie stattdessen als Windows-Administrator angemeldet, riskieren Sie Ihre Systemsicherheit.

Viele Nutzer verwenden Windows, während sie mit einem Administrator-Profil angemeldet sind. Dies birgt eine ganze Reihe an Risiken im Alltag, denn das System ist so anfällig für Viren, Trojaner und weitere Sicherheitsrisiken.

Oft reicht schon der simple Aufruf einer infizierten Internetseite oder E-Mail. Dies führt im schlimmsten Fall zum Befall Ihres Systems.

- Unerwünschte Programme könnten installiert werden.
- Ihre Dateien könnten gelöscht werden.
- Neue Benutzer mit administrativen Rechten könnten erstellt werden.
- ...und vieles mehr.

Microsoft empfiehlt, Ihren Computer ausschließlich als Benutzer zu verwenden:

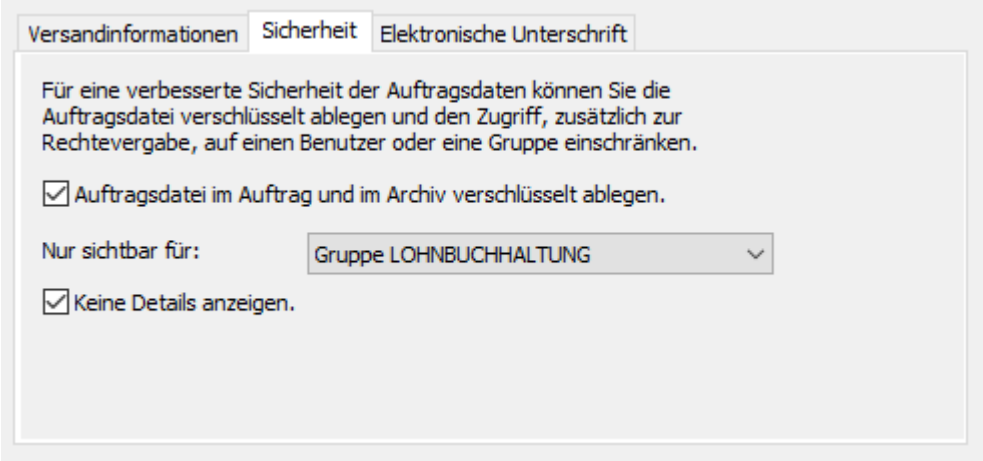
- Ihr Benutzer darf nicht Mitglied der Gruppe der **Administratoren** sein.
- Domänenbenutzerkonten dürfen ausschließlich der Gruppe **Benutzer** angehören.
- Tipp: benötigen Sie kurzzeitig administrative Rechte, nutzen Sie einfach die Funktion **"Als Administrator ausführen"**

2 Sicherheit innerhalb von SFirm erhöhen

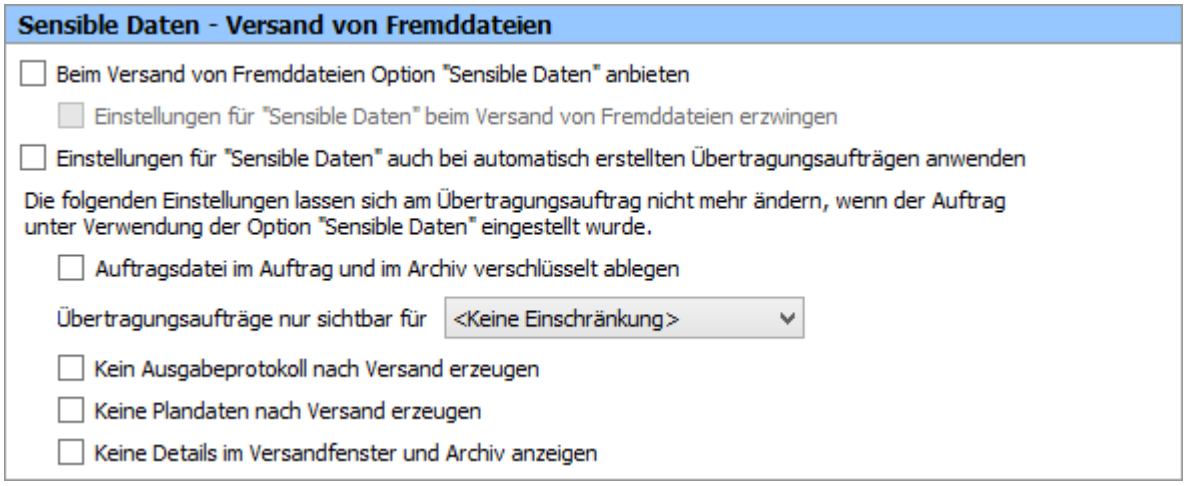
Um die Sicherheit ihrer Daten zu erhöhen und das Arbeiten mit SFirm noch komfortabler zu gestalten, bieten wir Ihnen innerhalb der Software verschiedene Einstellungsmöglichkeiten:

2.1 Arbeiten mit sensiblen Daten

Wenn Sie nicht möchten, dass einzelne Lohn- und Gehaltszahlungen oder andere Zahlungen in einem Übertragungsauftrag oder später im Archiv gesehen werden können, können Sie diese Zahlungen als *sensible Daten* kennzeichnen.
Sie können die *sensiblen Daten* bei jeder Ausgabe, also individuell für einen Sammler, über den Reiter „Sicherheit“ hinterlegen. Setzen Sie dazu den Haken bei „Auftragsdatei im Auftrag und im Archiv verschlüsselt ablegen“ und hinterlegen Sie möglichst eine Gruppe, die auf die sensiblen Daten zugreifen darf. Sollten Sie keine Gruppe oder keinen Benutzer hinterlegen, wird die Datei nicht verschlüsselt.
Über den Haken „Keine Details anzeigen“ steuern Sie, dass der nachfolgende Benutzer keine einzelnen Posten sehen kann, obwohl dieser auf die Datei zugreifen kann.

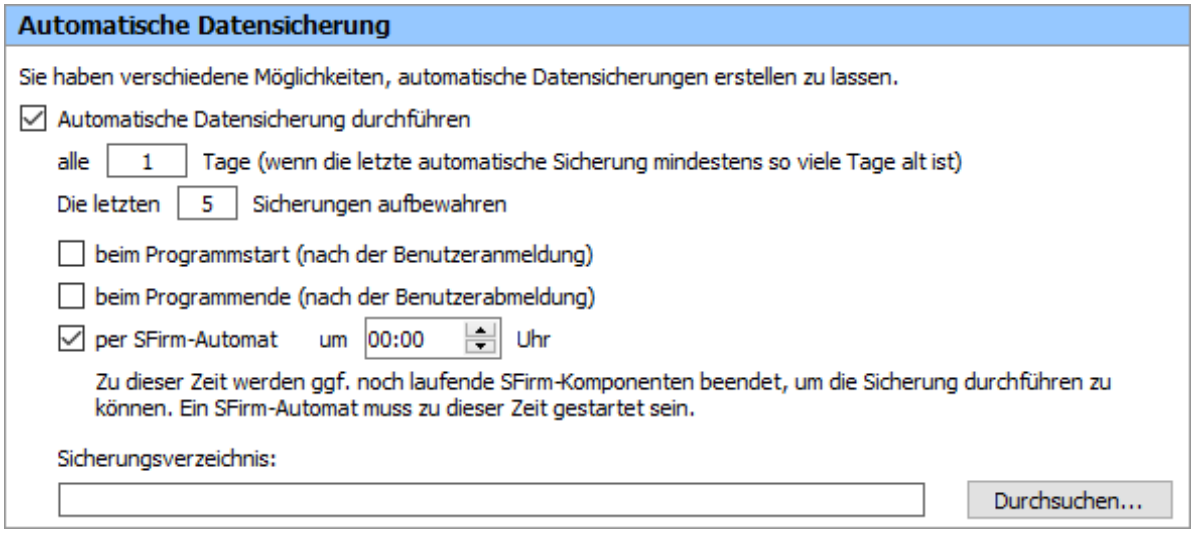


Generell können Sie die *sensiblen Daten* für Zahlungsverkehrsdateien aus fremden Produkten über die Einstellungen von SFirm hinterlegen. Sie entscheiden, ob die sensiblen Daten nur angeboten oder erzwungen werden bzw. bei automatisch aus Fremddateien erzeugten Übertragungsaufträgen immer angewendet werden.
Optional gibt es hier noch die Möglichkeit das Erzeugen des Ausgabeprotokolls und das Anlegen von Plandaten in der Datenbank zu verhindern.



2.2 Automatische Datensicherung

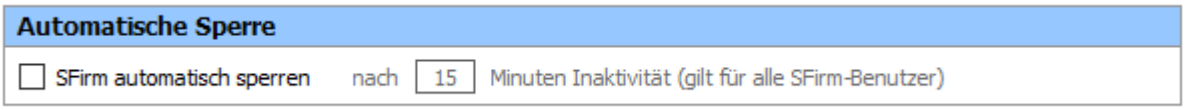
Auch wenn Ihre Server von der IT generell gesichert werden, macht es Sinn die Daten aus SFirm noch einmal separat zu sichern. So lassen sich kleinere Probleme wie ein versehentliches Löschen schnell beheben.
Hinterlegen Sie dazu in den Einstellungen von SFirm unter dem Punkt „Automatische Datensicherung“, ob und wann eine automatische Datensicherung durchgeführt werden und wo sie abgelegt werden soll. Definieren Sie auch wie häufig die Daten gesichert und wie viele alte Sicherungen aufbewahrt werden.



Soll die automatische Datensicherung zum Programmstart oder zum Programmende erzeugt werden, benötigt der erste bzw. letzte SFirm-Benutzer, der sich in SFirm an- bzw. aus SFirm abmeldet, das Recht „Daten sichern“. Im Zweifel sollten alle SFirm-Benutzer dieses Recht bekommen.

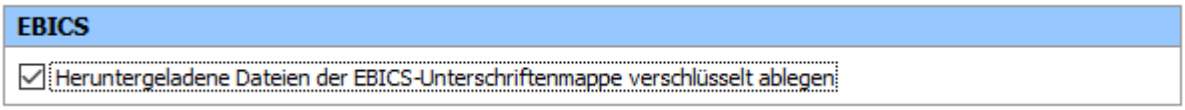
2.3 Automatische Sperre bei Inaktivität

Aus Datenschutzgründen kann SFirm nach einer vorgegebenen Zeit gesperrt werden. Zum Aktivieren von SFirm ist dann wieder das Kennwort des SFirm-Benutzers einzugeben.



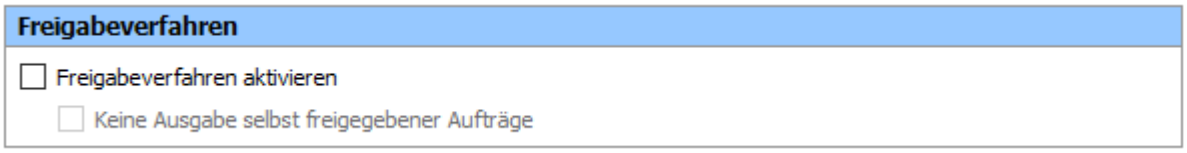
2.4 Dateien der EBICS-Unterschriftenmappe verschlüsselt ablegen

Dateien, die über die in SFirm integrierte Unterschriftenmappe abgeholt, also **heruntergeladen** wurden, lassen sich verschlüsselt ablegen. Dies ist in den Einstellungen von SFirm zu finden.



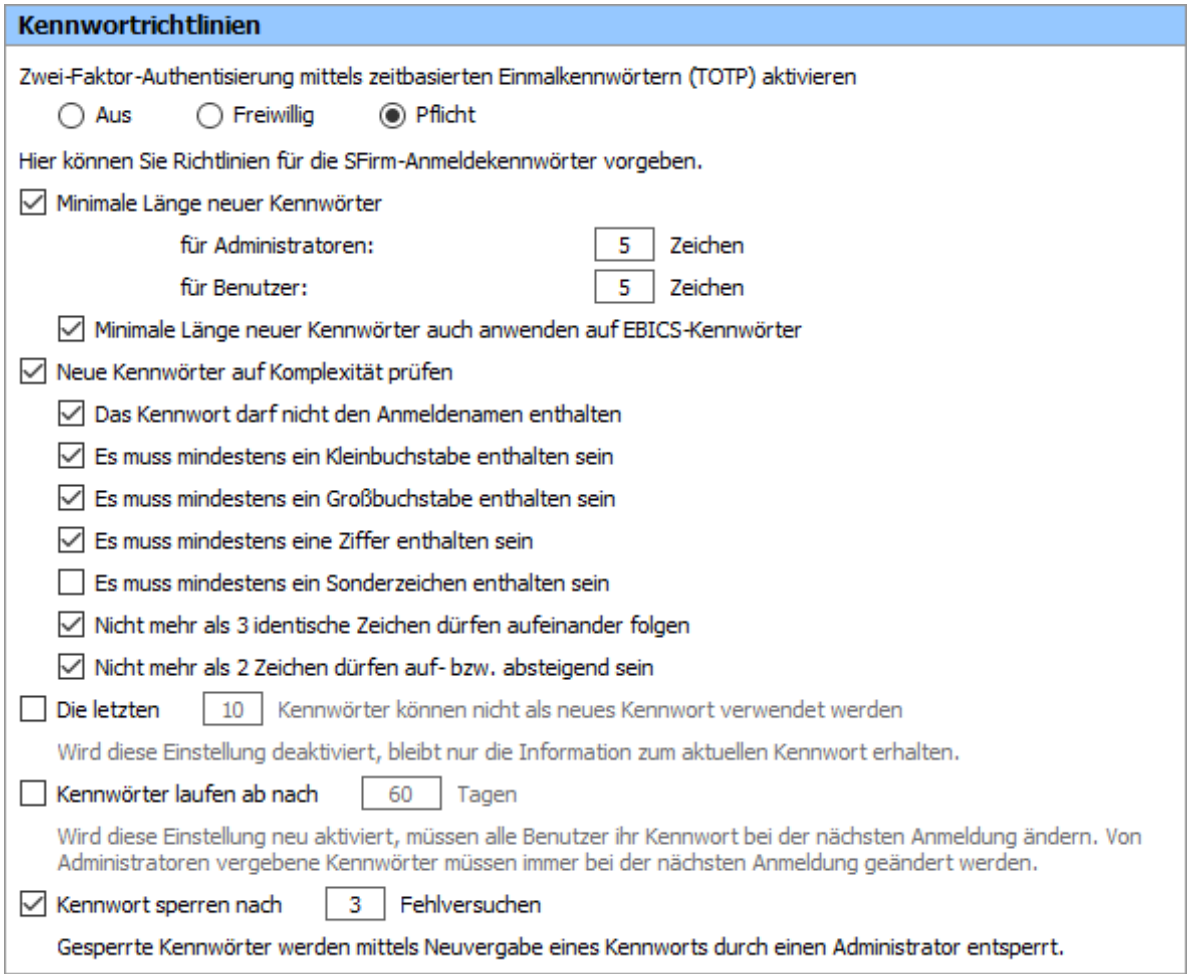
2.5 Das Freigabeverfahren

Es ist möglich neben den Sicherheitsmechanismen, die die Bankrechner zur Verfügung stellen, eine weitere Authentifikationsebene in SFirm zu nutzen, - das Freigabeverfahren. So kann es ein oder zwei Unterschriftsberechtigte geben, die der Bank bekannt sind und einen weiteren Benutzer, der nur freigibt.
Die Freigabe erfolgt vor dem Erzeugen der Übertragungsaufträge und vor dem Unterschreiben. Der freigebende Benutzer bestimmt also welche Zahlungen überhaupt in den Ausgabeprozess eintreten.
Dazu ist es nötig, das Freigabeverfahren generell in den Einstellungen zu erlauben und dem freigebenden Benutzer das Recht „Freigabe durchführen“ zu geben.



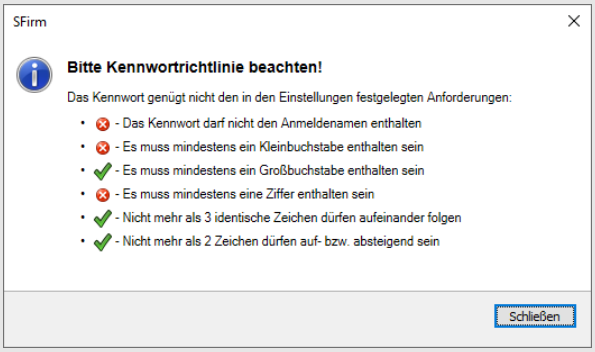
2.6 Kennwortrichtlinien

Um den gestiegenen Sicherheitsbedarf in Bezug auf die Login-Daten des Programms gerecht zu werden, gibt es die Gruppe *Kennwortrichtlinien*



Hier können verschiedene Einstellungen getätigt werden, um eine höhere Passwortkomplexität und/oder einen regelmäßigen Wechsel des Login-Passwortes zu erzwingen. Standardmäßig sind diese Einstellungen bei der Neuinstallation oder bei der Anlage eines neuen Mandanten aktiviert. Das war bei bestehenden Installationen nicht immer so. Sie sollten deshalb bei bestehenden Installationen prüfen, wie die Kennwortrichtlinien gesetzt sind. Die Prüfungen werden nur für das Zugangskennwort zum Programm durchgeführt. Die gewählten Regeln gelten auch für Administratoren. Änderungen können hier nur von Administratoren vorgenommen werden.

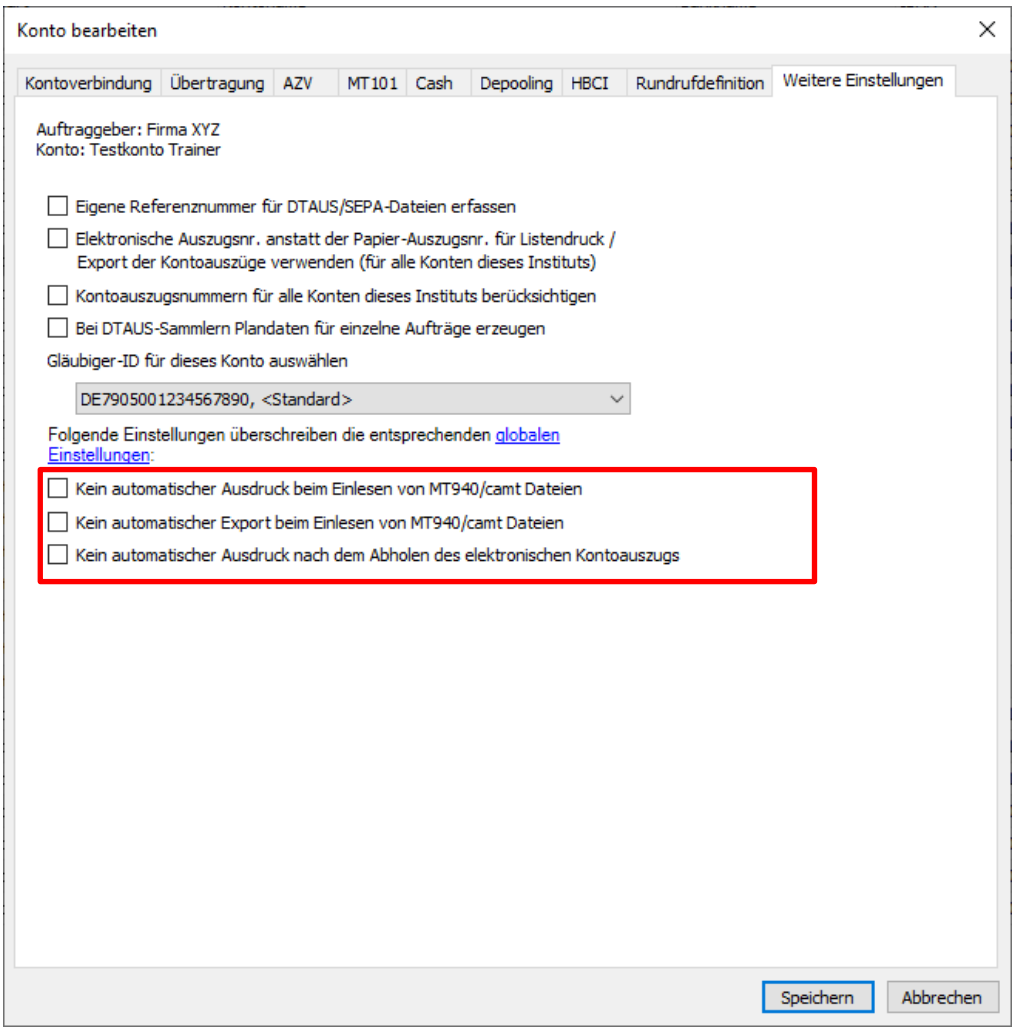
Hier können Sie Richtlinien für die SFirm-Anmeldekennwörter vorgeben.	
Zwei-Faktor-Authentisierung mittels zeitbasierten Einmalkennwörtern (TOTP) aktivieren [.] Aus [ ] Freiwillig [.] Pflicht	Ist die Zwei-Faktor-Authentisierung aktiv ist es entweder möglich (freiwillig) oder nötig (Pflicht) ein Einmalpasswort durch eine andere Applikation erzeugen zu lassen, um sich an diesem Mandanten anzumelden.

[ ] Minimale Länge neuer Kennwörter: [ ] Zeichen	Hiermit legen Sie die minimale Anzahl der Zeichen fest, die bei der Vergabe von neuen Anmeldekennwörtern in der Benutzerverwaltung eingegeben werden müssen. Wird diese Anzahl unterschritten, erhalten Sie die Meldung *Kennwort genügt nicht der Längenanforderung*. Dabei kann die minimale Anzahl der Zeichen für Benutzer und Administratoren separat eingegeben werden. Standardmäßig ist die Einstellung gesetzt und für Administratoren sind 16 Zeichen und für Benutzer 10 Zeichen eingetragen.
[ ] Minimale Länge neuer Kennwörter auch anwenden auf EBICS-Kennwörter	Diese Einstellung ist standardmäßig aktiviert, deshalb gilt die minimale Länge neuer Kennwörter nicht nur für das Kennwort bei der SFirm-Anmeldung, sondern auch für die Kennwörter im EBICS-Bereich.
[ ] Neue Kennwörter auf Komplexität prüfen	Wird die Komplexitätsprüfung aktiviert, werden die eingegebenen Kennwörter auf ihre Komplexität hin untersucht. Kennwörter, die z.B. aus dem Benutzernamen oder identischen Zeichen bestehen, werden mit der folgenden Meldung abgewiesen: 
[ ] Die letzten [ ] Kennwörter können nicht als neues Kennwort verwendet werden	Mit dieser Einstellung weisen Sie SFirm an, sich (entsprechend der angegebenen Anzahl) die zuletzt vergebenen Kennwörter eines jeden Benutzers zu merken. Bei dem Versuch, ein in der Vergangenheit verwendetes Kennwort erneut zu hinterlegen, wird die Eingabe entsprechend abgewiesen. Wurde diese Einstellung verwendet und dann wieder deaktiviert, bleiben nur die Informationen zum aktuellen Kennwort der in der Benutzerverwaltung hinterlegten Benutzer erhalten.
[ ] Kennwörter laufen ab nach [ ] Tagen	Hiermit legen Sie die Gültigkeitsdauer aller in der SFirm-Benutzerverwaltung hinterlegten Kennwörter fest. Nach Ablauf der Anzahl Tage erscheint beim Programmstart eine Hinweismeldung, die die Eingabe eines neuen Kennwortes verlangt:
[ ] Kennwort sperren nach [ ] Fehlversuchen	Nach der angegebenen Anzahl von Fehlversuchen, schließt sich automatisch SFirm und das Kennwort des jeweiligen Benutzers, mit dem eine Anmeldung erfolgen sollte, wird gesperrt. Anschließend ist der Zugang nur über einen Administrator-Account zugänglich. Dieser kann dann wieder ein gültiges Kennwort für den betreffenden Benutzer vergeben.

Die Einstellungen in der Gruppe *Kennwortrichtlinien* haben nicht nur Auswirkungen auf neu angelegte, sondern auch bei der Änderung vorhandener Kennwörter.

2.7 Kontobezogene Einstellungen

Sie können in den Einstellungen von SFirm festlegen, dass die Umsätze oder der elektronische Kontoauszug generell für alle Konten gedruckt oder die Umsätze in ein selbst gewähltes Verzeichnis exportiert werden. Über die individuellen Einstellungen im Auftraggeber-Konto, können Sie diesbezüglich Ausnahmen für das jeweilige Konto definieren.
Für jedes Auftraggeber-Konto kann somit individuell festlegt werden, ob ein automatischer Ausdruck der Kontoumsätze, ein automatischer Export der Umsätze oder ein automatischer Ausdruck des elektronischen Kontoauszugs erfolgen soll.



2.8 Hinterlegung von Passwörtern/PINs

Das Hinterlegen von Passwörtern und PINs macht für automatisierte Vorgänge wie einen terminierten Rundruf Sinn. Andernfalls ist z.B. das nächtliche Abholen der Umsätze nicht möglich.

Übertragung per HBCI/FINTS

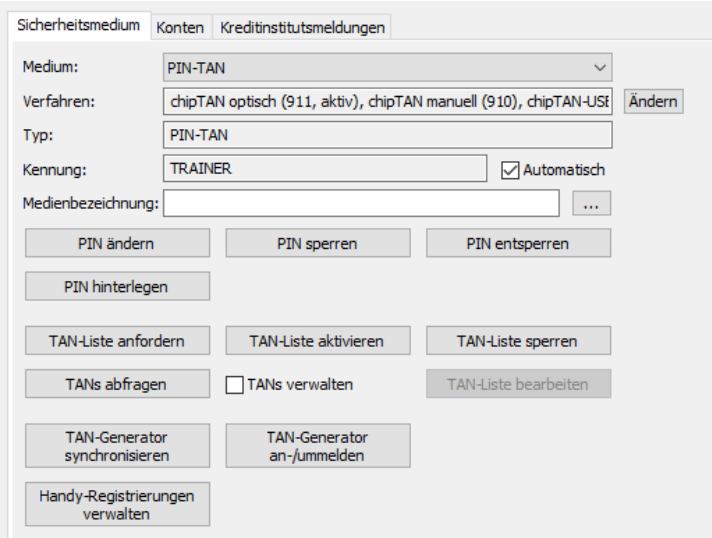
Im HBCI-Bankzugang lässt sich die PIN bzw. das Passwort hinterlegen. Es werden entsprechende Schaltflächen angezeigt.

Stammdaten ▸ Bankzugänge ▸HBCI ▸Benutzer

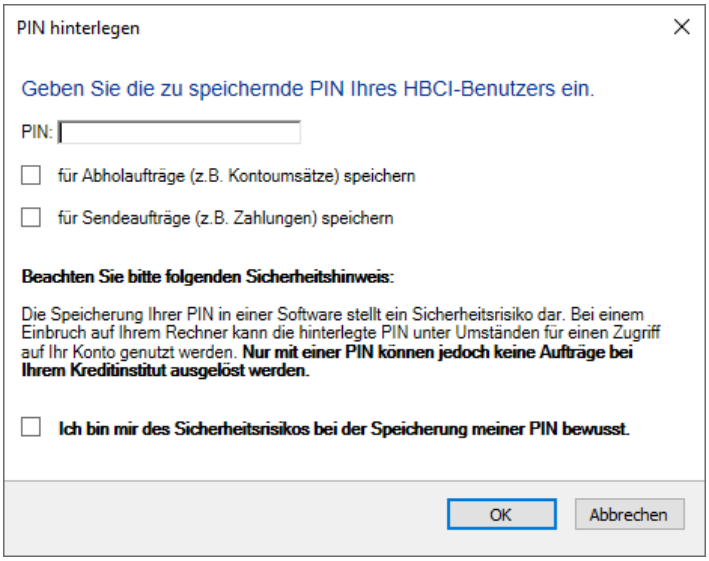
2.8.1 PIN/TAN-Verfahren

<PIN hinterlegen>

Hier haben Sie die Möglichkeit die PIN zu speichern. Sie bestimmen wie die hinterlegte PIN verwendet werden soll.

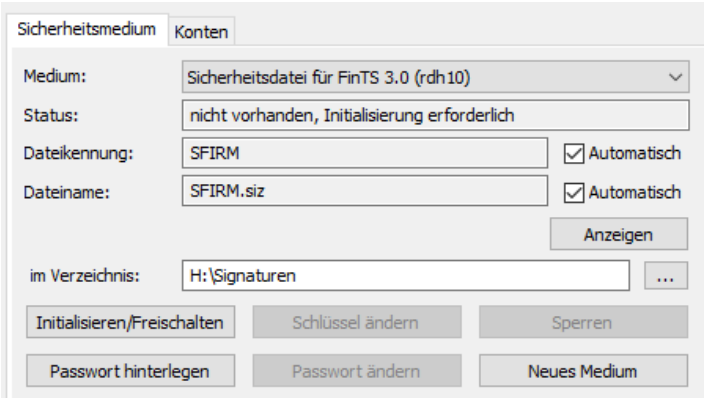


Die PIN kann **nur für Abholaufträge** oder **nur für Sendeaufträge** oder **für beide** verwendet werden.



2.8.2 Sicherheitsdatei

<Passwort hinterlegen>
den meisten Zugriffen auf eine Sicherheitsdatei ist eine vorherige Eingabe des Passworts durch den Benutzer erforderlich. Diese Prozedur entfällt, wenn das Passwort hinterlegt wird. **Allerdings besteht dann die Gefahr einer unbefugten Benutzung des Mediums**



2.8.3 Übertragung per EBICS

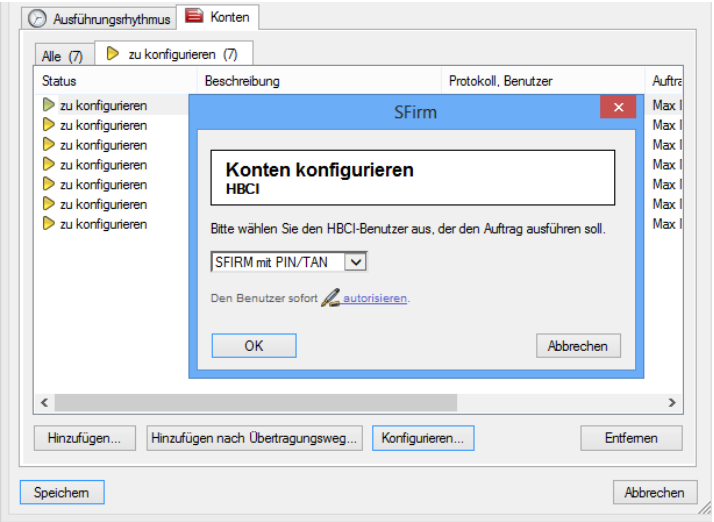
In EBICS wurde das Konzept des *technischen Teilnehmers* eingeführt, um den Komfort zu erhöhen und zeitversetztes, automatisiertes Versenden zu ermöglichen.

> Ein technischer Teilnehmer verwendet zur Signatur und Authentifikation fest im Programm hinterlegte Schlüssel und ist nicht berechtigt, bankfachliche Signaturen (echte elektronische Unterschriften) zu Sendeaufträgen zu leisten - er darf nur Daten transportieren.

Der grundlegende Unterschied im Vergleich zum normalen EBICS-Benutzer ist, dass die gesamten Sicherheitsfunktionen (EU, Authentifikationsschlüssel, Kennwörter) gespeichert werden dürfen und automatisch bei der Übertragung zugesteuert werden können. Damit diese Funktion nicht missbraucht werden kann, muss der *technische Teilnehmer* auf dem Bankrechner für alle verwendeten Auftragsarten eine T-Berechtigung besitzen. Innerhalb von EBICS kann ein fachlicher EBICS-Benutzer oder sogar SFirm selbst (bei automatischem Versand) die Sicherheitsmerkmale des *technischen Teilnehmers* bei der Kommunikation verwenden. Wichtig ist in diesem Zusammenhang, dass bei einer Einreichung von Aufträgen sowohl der Einreicher des Auftrags (also der fachliche Teilnehmer) als auch der Überträger des Auftrags (z.B. der technische Teilnehmer) im Bankprotokoll sichtbar werden und damit eine Nachvollziehbarkeit gegeben ist. Der EBICS-Standard sieht vor, dass das Endkundensystem selbst (also hier SFirm) als *technischer Teilnehmer* agieren kann. Das kann aus formalen Gründen beim Bankrechner so nicht eingetragen werden. Im Bankrechner muss ja eine EBICS-Kennung immer einer *natürlichen Person* zugeordnet sein. Es bietet sich in diesem Zusammenhang an, einen 'normalen' Teilnehmer (z.B. die Geschäftsführerin) mit einer zusätzlichen EBICS-Kennung auszustatten. Diese Teilnehmerin würde dann auch die INI-Briefe unterschreiben.

2.8.4 Hinterlegung des Passwortes oder der PIN im Rundruf

Markieren Sie die Konten, die Sie konfigurieren möchten und klicken Sie auf <Konfigurieren>. Wurden Konten gewählt, bei denen mindestens ein Übertragungsweg konfiguriert ist, erscheint der Konfigurationsdialog, in dem der HBCI oder EBICS-Benutzer festgelegt werden muss. Es kann pro Konto ein anderer Benutzer ausgewählt werden oder ein gemeinsamer für alle Konten. An dieser Stelle kann bereits die Autorisierung hinterlegt werden.



3 Übertragung allgemein

In SFirm kann mit den beiden Übertragungswegen HBCI/FINTS und EBICS gearbeitet werden. Außerdem ist es möglich das Browserbanking zu nutzen, also die Internetseite der Bank über SFirm aufzurufen.
Da gerade in Netzwerken Schutzmechanismen wie Virenscanner, Firewall, und Proxy-Server sind, müssen Windows-Ports bzw. Adressen im Internet separat freigegeben werden. Hier eine Zusammenstellung aller von SFirm genutzten Ports und Adressen. **Hinzu kommen noch die Adressen der Bankrechner.**

3.1 Generell freizugebende Adressen und Ports

Für das Versionsupdate, die Serviceupdates, Premium Message, Konfiguration und Lizenzmanagement sind folgende Adressen und Ports freizugeben:

Freigeschaltete Adressen	• www.sfirm.de • download.sfirm.de • downloads.starfinanz.de (CDN, daher keine statische IP verfügbar) • services.starfinanz.de • finanzcockpit.starfinanz.de
Freigeschaltete Ports	• 53 (DNS Nameservice) • 80 (http) • 443 (https)

In den Internetoptionen des Internet Explorers ▸ Erweitert, müssen die TLS-Checkboxen aktiviert sein. Alternativ bitte die Standardeinstellungen wiederherstellen.

3.2 MS SQL Server

Freigeschaltete Ports	• 1433 TCP • 1434 UDP (Nur bei SQL Express)

3.3 Browser Banking

Anschluss & Zugang	• Eine funktionsfähige Internetanbindung (TCP/IP).
Freigeschaltete Ports	• 53 (DNS Nameservice) zur Namensauflösung der Rechneradressen im Internet • 80 (http) • 443 (https)

3.3 EBICS

Anschluss & Zugangsdaten	• Eine funktionsfähige Internetanbindung (TCP/IP). • Bei Autorisierung mit Chipkarte: Chipkartenlesegerät mit PC/SC oder CT-API (Software) und eine freie Schnittstelle. • Anmeldung und Einrichtung des Kunden beim Rechenzentrum. • Mitteilung des Instituts mit den EBICS-Teilnehmerdaten.
Freigeschaltete Ports	• 53 (DNS Nameservice) zur Namensauflösung der Rechneradressen im Internet • 80 (HTTP) • 443 (HTTPS)

3.4 HBCI mit Chipkarte

Hardware & Treiber	• Eine funktionsfähige Internetanbindung (TCP/IP). • Bei Autorisierung mit Chipkarte: Chipkartenlesegerät mit PC/SC oder CT-API (Software) und eine freie Schnittstelle. • Anmeldung und Einrichtung des Kunden beim Rechenzentrum. • Verbindungsdaten für Institut/Bank (i.d.R. auf Chipkarte).
Freigeschaltete Ports	• 53 (DNS Nameservice) zur Namensauflösung der Rechneradressen im Internet • 80 (HTTP) • 3000 (PPP)

3.5 HBCI mit PIN/TAN

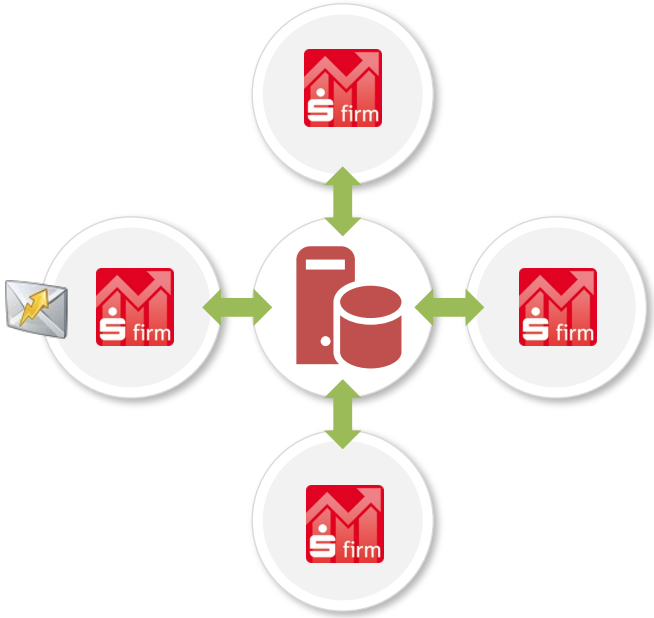
Anschluss & Zugangsdaten	• Eine funktionsfähige Internetanbindung (TCP/IP). • Bei Autorisierung mit Chipkarte: Chipkartenlesegerät mit PC/SC (Software) und eine freie Schnittstelle. • Anmeldung und Einrichtung des Kunden beim Rechenzentrum. • Autorisierung mit PIN/TAN: PIN und TAN.
Freigeschaltete Ports	• 53 (DNS Nameservice) zur Namensauflösung der Rechneradressen im Internet • 80 (HTTP) • 443 (https)

⚠ Bitte beachten Sie, dass SFirm derzeit nicht mit IPv6-only Netzwerken kompatibel ist. Da einige Kunden ausschließlich IPv6-only einsetzen, sollten sie auf diesen Umstand vor einem SFirm-Einsatz hingewiesen werden.

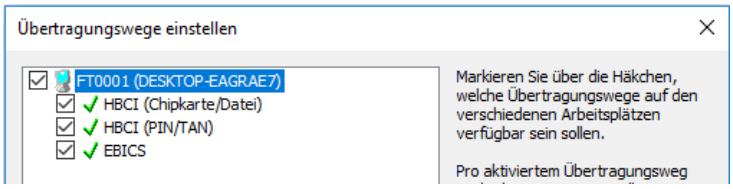
3.6 Einsatz angepasster Netzwerkumgebungen

3.6.1 Übertragungsserver

Während im Normalfall jeder Client die Übertragung an den Bankrechner selbst mithilfe des *SFAutomat* vornimmt, kann die Aufgabe auch ein Server übernehmen, um die Sicherheit zu steigern. Ein Server-Betriebssystem lässt sich immer besser gegen Angriffe schützen als ein Client.
Auf den Arbeitsstationen ist **keine** LAN- oder Einwahl-Verbindung verfügbar. Nur eine (ggfs. mehrere) Arbeitsstation macht die **Übertragung für alle** mit dem SFirm-Automaten.



Im Menüband „Wartungscenter“ müssen die **Übertragungswege** auf dem Übertragungsserver aktiviert und konfiguriert werden, die Übertragungen machen sollen.
Auf allen anderen Arbeitsstationen dürfen sie nicht aktiviert sein, bzw. müssen deaktiviert werden.



3.6.2 Einsatz von Remotedesktopservern und Citrix Server

Da bei Remotedesktopservern bzw. Terminalservern, wie sie früher hießen, oder Citrix-Servern nur Bilddaten übertragen werden, die eigentliche Rechenarbeit aber auf dem Server selbst passiert, ist auch das Einbinden anderer Standorte recht unproblematisch.
Durch das Bereitstellen einer Anwendung vom Server aus durch die IT hat der Anwender auf seinem Client wenig Möglichkeiten die Systemumgebung zu beeinflussen.

Natürlich werden sowohl Remotedesktopserver von Microsoft wie die entsprechenden Produkte von Citrix von SFirm unterstützt. Genaueres entnehmen Sie bitte unseren aktuellen Systemvoraussetzungen. http://www.sfirm.de/system-requirements.html

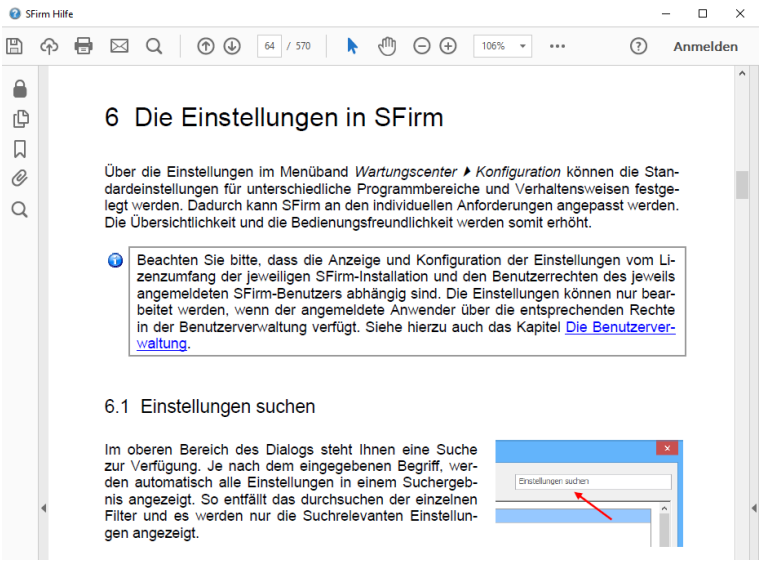
4 Weitere Informationsquellen & Support

Neben dem Kundenhandbuch und den Kundenleitfäden stellen die Hilfe und die Inhalte des Internetauftritts www.sfirm.de weitere Quellen dar, Informationen rund um SFirm zu erhalten. Mit den angebotenen Seminaren haben Sie außerdem die Möglichkeit, themenbezogen das eigene Wissen in Theorie und Praxis zu vertiefen. Zusätzlich dazu hilft Ihnen der technische Kundenservice des Herstellers bei allen technischen Fragen und Problemen. Im letzten Abschnitt finden Sie alle Kontaktdaten im Überblick.

4.1 Die Hilfe in SFirm

Die Hilfe ist ein Bestandteil der Anwendung SFirm. Sie ist mit den jeweiligen Programmteilen bzw. Funktionen verbunden und zeigt Ihnen – je nachdem, wo Sie sich gerade befinden – nach dem Aufruf mit der F1-Taste die entsprechend zugehörige Beschreibung und Hilfe an.

Die Hilfe ist überwiegend nach Programmbereichen und Programmfunktionen strukturiert und gibt Ihnen somit auch die Möglichkeit, sich über diese Hilfe in SFirm einzuarbeiten.

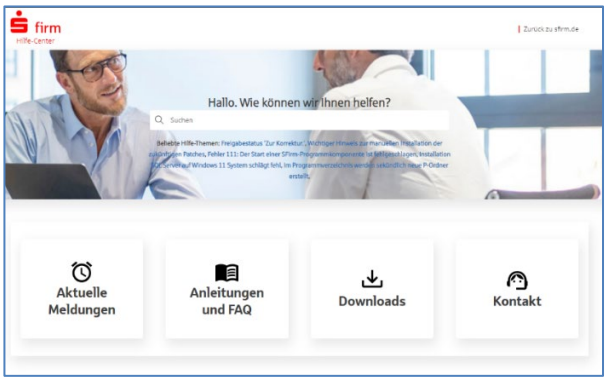


4.2 Der Internetauftritt von SFirm

Über die Adresse www.sfirm.de haben Sie einen Zugang zum SFirm-Internetauftritt. Die SFirm-Website ist in zwei Bereiche eingeteilt: einen allgemein zugänglichen Teil, der auch den Großteil der aktuellen Informationen zu den Produkten und Modulen enthält und einen exklusiven Bereich für die Berater der Sparkassen und Landesbanken. Im öffentlichen Teil sind mehrere Rubriken zu sehen, über die Sie aktuelle Informationen, Leitfäden, Modulbeschreibungen und Schulungsangebote sowie Downloads von Updates und Tools erreichen können.

4.2.1 SFirm Hilfe-Center

Das SFirm Hilfe-Center enthält eine Wissensdatenbank, die Informationen, Hinweise und Problemlösungen zu den aktuellen, freigegebenen Versionen von SFirm strukturiert zur Verfügung stellt. Alle Informationen finden Sie auf hilfe.sfirm.de.



4.2.2 Seminare

Für SFirm bieten wir Ihnen eine Reihe von Seminaren an, die sich an unterschiedliche Zielgruppen wendet. Eine Auflistung der derzeit angebotenen Seminare erhalten Sie über den SFirm-Internetauftritt www.sfirm.de in der Rubrik *Seminare*. Für nähere Informationen steht Ihnen auch unser Seminar-Team telefonisch und per E-Mail zur Verfügung (siehe übernächsten Abschnitt).

4.3 Der technische Kundenservice

Der Hersteller bietet Ihnen einen kostenpflichtigen technischen Support für alle SFirm-Produkte an. Detaillierte Informationen finden Sie auf der Seite www.sfirm.de in der Rubrik *Kontakt*. Die SFirm-Hotline steht Ihnen von montags - freitags von 8:00 bis 20:00 Uhr unter folgender kostenpflichtigen Rufnummer zur Verfügung:

0900 / 71 55 99 0 (2,49 EUR/Minute inkl. MwSt. aus dem dt. Festnetz; abweichende Preise für Mobilfunkteilnehmer).

4.4 Kontaktinformationen

Folgende Tabelle gibt Ihnen einen Überblick über die wichtigsten Kontaktdaten des Herstellers:

Anschrift		Star Finanz-Software Entwicklung und Vertriebs GmbH Grüner Deich 15 20097 Hamburg
Internetauftritte:	Produktseite Firmenseite	www.sfirm.de www.starfinanz.de
Vertrieb Rufnummer		040 / 23728 - 333
Vertrieb Fax		040 / 23728 - 166
Vertrieb E-Mail		vertrieb@starfinanz.de
Technische Hotline für Endkunden		0900 / 71 55 99 0 (2,49 EUR/Minute inkl. MwSt. aus dem deutschen Festnetz; abweichende Preise für Mobilfunkteilnehmer).