

Dokument opisuje system bezpieczeństwa (kontroli przed niepowołanym dostępem) w systemie AlfaSprzedaż

Dokument opisuje sposoby zabezpieczenia danych systemu AlfaSprzedaż przed niepowołanym dostępem. Dostępne są dwa zabezpieczenia:

a) zabezpieczenie przed dostępem do programu AlfaCentrala, lub innym dostępem do danych znajdujących się w bazie centralnej systemu AlfaSprzedaż,

b) zabezpieczenie przed niepowołanym dostępem do serwera Mobilink.

Oba mechanizmy oparte są o system haseł.

Ustanowienie hasła dostępu do programu AlfaCentrala

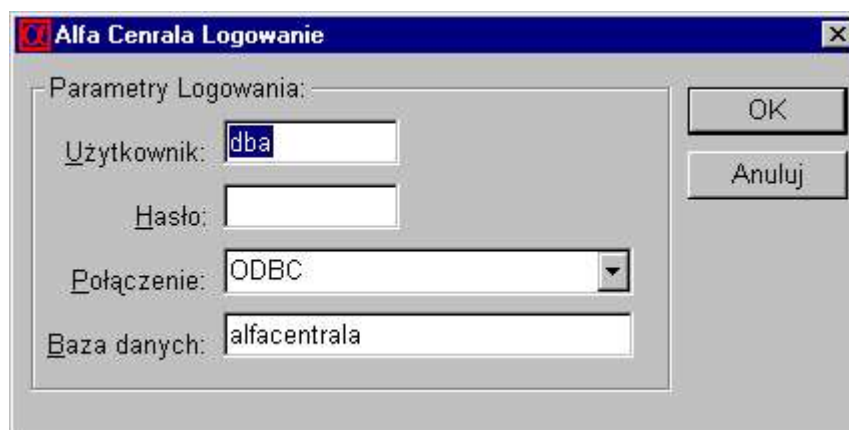
AlfaCentrala korzysta z systemu bazodanowego SQL Anywhere firmy Sybase Inc. Baza ta przechowywana jest fizycznie w pliku {katalog instalacji}\data\alfacentrala.db.

Zarówno AlfaCentrala jak i serwer Mobilink (serwer synchronizacji), przy starcie łączą się z bazą alfacentrala.db za pośrednictwem źródła ODBC o nazwie "AlfaCentrala". To źródło instalowane jest automatycznie przez program instalacyjny AlfaSprzedaży. Drajwer ODBC jest nazwany "Alfa Centrala ASA 7.0", w rzeczywistości jest to standardowy drajwer SQL Anywhere 7, o nieco zmienionej nazwie.

Bezpośrednio po instalacji systemu AlfaSprzedaż, wszystkie programy logują się do bazy automatycznie. W rzeczywistości dostęp do bazy SQL Anywhere odbywa się po podaniu nazwy użytkownika i hasła dostępu. Bezpośrednio po instalacji AlfaCentrala oraz wszystkie programy systemu łączą się do bazy automatycznie jako użytkownik **DBA** z hasłem **SQL**.

Aby wymusić podanie hasła "SQL" przy logowaniu do programu AlfaCentrala (wielkość liter nie ma znaczenia, hasło może też być podane małymi literami) należy zmienić wartość parametru "AutoConnect" znajdującego się w pliku "{katalog instalacji}\exe\alfa.ini w sekcji [Application Parameters] na wartość 0.

Wtedy każdorazowo przy uruchamianiu programu AlfaCentrala będzie się pojawiało okienko logowania



W którym w polu "hasło" należy wpisać hasło "SQL".

To jednak oczywiście nie uniemożliwia dostępu osobom, które znają domyślne hasło dostępu do programu AlfaSprzedaż.

Aby można było uniknąć ryzyka niepowołanego dostępu konieczna jest zmiana samego hasła użytkownika DBA.

Firma ApSys celowo nie dostarcza prostej metody zmiany tego hasła (tylko nieco bardziej skompilowaną opisaną poniżej). Powodem jest zapewnianie, że użytkownik zmieniający hasło

dostępu do bazy danych jest doświadczonym użytkownikiem systemu i jest świadomy konsekwencji zapomnienia takiego zmienionego hasła.

Konsekwencją zapomnienia zmienionego hasła użytkownika DBA jest niemożność dostępu do danych bazy AlfaCentrali i konieczność cofnięcia się do ostatniego backupu bazy sprzed zmiany hasła lub reinstalacja całego systemu.

Aby zmienić hasło użytkownika DBA należy uruchomić program dbmsqlc dostarczany w katalogu {katalog instalacji}\asa\, zalogować się na użytkownika DBA z podaniem dotychczasowego hasła, a następnie w oknie command wpisać polecenie:

```
GRANT CONNECT TO DBA IDENTIFIED BY moje_nowe_haslo;
```

i nacisnąć przycisk “Execute”

Po zmianie hasła uruchomienie programu AlfaCentrala będzie możliwe wyłącznie z użyciem okienka logowania, po podaniu prawidłowego hasła.

Po zmianie hasła użytkownika DBA konieczna jest też modyfikacja skrótu uruchamiającego serwer Mobilink.

Przykładową linię startu serwera Mobilink:

```
"c:\Program Files\AlfaS\asa\dbmslrv7.exe" -x tcpip{keep_alive=1} -o "D:\Program Files\AlfaS\ml\ml.log" -v -c "dsn=AlfaCentrala;uid=dba;pwd=sql"
```

zmieniamy na

```
"c:\Program Files\AlfaS\asa\dbmslrv7.exe" -x tcpip{keep_alive=1} -o "D:\Program Files\AlfaS\ml\ml.log" -v -c "dsn=AlfaCentrala;uid=dba;pwd=moje_nowe_haslo"
```

Alternatywną metodą zapewniającą największe możliwe bezpieczeństwo systemu jest zupełne usunięcie hasła z tej linijki:

```
"c:\Program Files\AlfaS\asa\dbmslrv7.exe" -x tcpip{keep_alive=1} -o "D:\Program Files\AlfaS\ml\ml.log" -v -c "dsn=AlfaCentrala;uid=dba"
```

i wpisanie nowego hasła w źródle ODBC “Alfacentrala”. W tym celu uruchamiamy program ODBC Administrator i w zakładce “System DSN” wskazujemy źródło “AlfaCentrala” i naciskamy “Configure”, po czym w zakładce “login” w polu “hasło” wpisujemy nowe hasło (np “**moje_nowe_haslo**”) i naciskamy OK.

Ustanowienie hasła dostępu aplikacji mobilnej do serwera synchronizacji

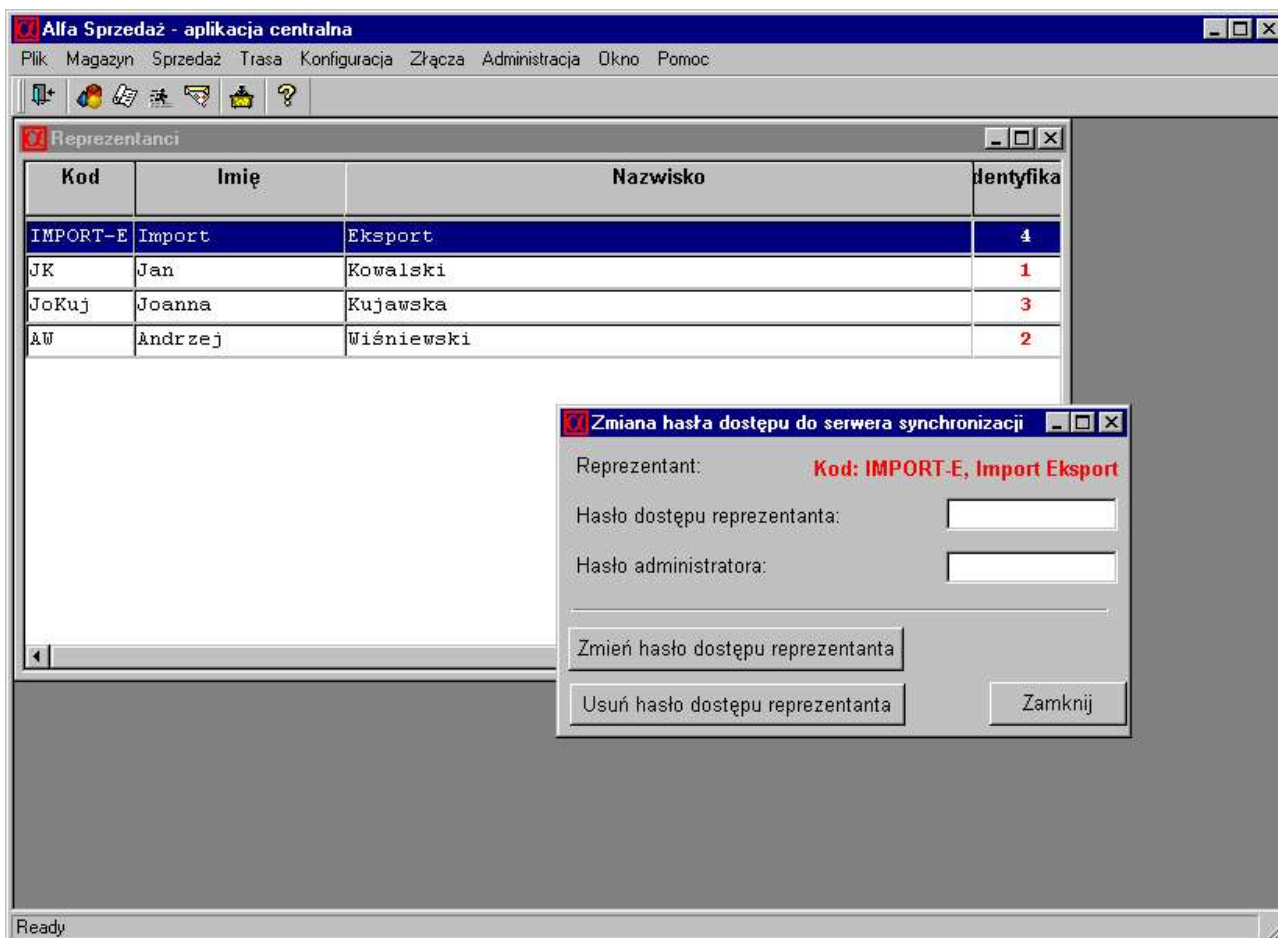
Użytkownik zdalny łączy się z bazą centralną za pośrednictwem serwera Mobilink. Każdy z palmtopów ma przypisany numer (identyfikator synchronizacji), według którego rozpoznawany jest palmtop. Ten mechanizm może być potencjalnie niebezpieczny, gdyż po pierwsze możliwa jest pomyłka i przydzielenie dwóm palmtopom tego samego numeru przez co dojdzie do rozsynchronizowania danych w bazie, po drugie brak jest jakiegokolwiek osłony przed próbą

zsynchronizowania się włączywacza posiadającego system AlfaSprzedaż.

Zabezpieczniem przed taką sytuacją jest włączenie mechanizmu autentykacji użytkowników zdalnych nie tylko przez numery ale także przez hasła.

Użytkownik zdalny podaje przy synchronizacji swój hasło dostępu a serwer synchronizacji sprawdza, czy hasło jest zgodne z zapisanym w bazie centralnej.

Aby uruchmić system autentykacji w oparciu o hasła potrzebne jest przestawienie parametru aplikacji mobilnej o nazwie "Poziom bezpieczeństwa systemu" na wartość 1 (lub większą) . Po uruchmieniu systemu autentykacji dokonujemy kolejnej synchronizacji wszystkich palmtopów przedstawicieli (spowoduje to przesłanie nowej konfiguracji na palmtopy), a następnie w AlfaCentrali otwieramy okienko z listą reprezentantów i na liście zmieniamy kolejno hasła dostępu poszczególnych przedstawicieli:



Hasło administratora to hasło użytkownika DBA, domyślnie "SQL".

Przy kolejnej próbie synchronizacji reprezentant będzie musiał podać hasło dostępu do serwera synchronizacji wpisując je w okienku na palmtopie, które pojawi się przy próbie synchronizacji danych.



Jeżeli reprezentant resynchronizuje dane i kasuje swoją bazę z palmtopa, to zachodzi konieczność usunięcia hasła reprezentanta korzystając z pokazanego wyżej okienka i przycisku “Usuń hasło dostępu reprezentanta”. Jest tak dlatego, że pierwsza synchronizacja (synchronizacja przy pustej bazie na palmtopie) odbywa się bez użycia hasła.

Uwaga! Przy wykasowanym hasle reprezentanta w AlfaCentrali serwer synchronizacji nie weryfikuje hasła użytkownika zdalnego podczas synchronizacji.

W przypadku gdy użytkownik poda błędne hasło zgłoszony zostanie komunikat “Błąd bazy danych -103”.

Będzie też komunikat w logu serwera synchronizacji ({katalog instalacji}\ml\ml.log)

E. dd/mm hh:mm:ss. [{nr}]: Error: Invalid password for user {nr}.

Adam Kujawski