

Włączenie szyfrowanych połączeń

Porada dla zakładów fotograficznych - dotyczy programu diPhoto Network

Informacje ogólne

diPhoto Home może komunikować się z internetem stosując bezpieczne protokoły komunikacyjne SFTP i HTTPS. Dzięki temu firmy obawiające się, że jakiś zaawansowany klient podejrzy dane potrzebne do dostępu do FTP firmy mogą włączyć taką bezpieczną komunikację i w ten sposób praktycznie zlikwidować takie niebezpieczeństwo. Dzieje się to kosztem zmniejszenia szybkości transmisji danych. Testy wykazały że transfer może się zmniejszyć o ok. 10-30%.

Włączenie bezpiecznej komunikacji diPhoto Home z Internetem wykonuje się poprzez

- wejście do diPhoto Network/Kioski, Wzorcowy kiosk Home Ordering, Ustawienia
- zmianę http na https w Pozostałe/Płatności/opcja Serwer
- włączenie Ogólne/Firma i kiosk/przycisk Ustawienia FTP/opcja SFTP
- wysłanie aktualizacji na FTP za pomocą diPhoto Network/Aktualizacje

Uwagi

- *Trzeba pamiętać, że w firmach stosujących bezpieczną komunikację w diPhoto Home firm.ini dla diPhoto Home różni się od firm.ini dla diPhoto Network i Point.*
- *Program został zmodyfikowany tak, że firm.ini dla centrali generuje się w diPhoto Network/Ustawienia/ Ogólne/Firma i kiosk/przycisk Generuj natomiast firm.ini dla diPhoto Home generuje się w diPhoto Network/Kioski/wybrać kiosk Wzorcowy Home Ordering/przycisk Ustawienia/Ogólne/Firma i kiosk/przycisk Generuj. Należy zdawać sobie sprawę z tego, że żeby bezpieczna komunikacja była możliwa nie wystarczy nowy program i włączenie odpowiednich opcji. W pierwszej kolejności serwer FTP i HTTP musi umożliwiać taką komunikację.*