BMS

Wymagania techniczne związane z wdrożeniem

Data dokumentu: 2017-11-15

SoftVig Systemy Informatyczne Sp. z o.o.

Ul. Cyfrowa 4, 71-441 Szczecin, tel. +48 91 350 89 20, fax +48 91 350 89 30

www.softvig.pl, e-mail: office@softvig.pl

Spis treści

1 Wprowadzenie

BMS jest aplikacją służącą do zarządzania procesami zachodzących w dziale napraw blacharsko-lakierniczych.

2 Architektura systemu

Niniejszy dokument definiuje wymagania sprzętowe oraz konfiguracyjne do spełnienia przez Zakład dealerski w celu uzyskania gotowości do wdrożenia technicznego aplikacji BMS.

Program jest dostępny z poziomu przeglądarki internetowej i dostosowany do pracy na komputerze stacjonarnym oraz na urządzeniu mobilnym - tablecie. Moduł blacharski współpracuje z systemem DMS AutoStacja3 dealera oraz z platformą internetową AudaNet.

Elementy architektury BMS:

- Serwer aplikacyjny IIS dealera.
- Serwer SQL dealera.
- DMS AutoStacja3.
- Sieć Wi-Fi dealera (dla urządzeń mobilnych).
- Stanowiska komputerowe dealera.
- Urządzenia mobilne pracujące w sieci Wi-Fi dealera.
- Ekran/Telewizor (wyświetlanie tablicy planowania napraw na warsztacie).

2.1 Część kliencka

Urządzenia, na których będzie uruchamiany system BMS muszą posiadać dostęp za pomocą protokołu https do aplikacji BMS. Adres internetowy, pod którym będzie dostępna aplikacja BMS będzie subdomeną w domenie svcloud.pl (dedykowana nazwa). Stacje robocze muszą również komunikować się z witryną (zabezpieczoną certyfikatem SSL) na serwerze IIS dealera w celu współpracy z systemem DMS AutoStacja 3.

2.2 Część serwerowa

System BMS do współpracy z DMS AutoStacja3 wymaga serwera IIS.

2.2.1 IIS, Certyfikat SSL

Ze względów bezpieczeństwa komunikacja pomiędzy urządzeniami a systemem DMS odbywa się za pomocą protokołu https. W związku z tym na serwerze IIS w Zakładzie dealerskim musi być zainstalowany certyfikat SSL o wymaganiach:

- Certyfikat publiczny
- Certyfikat podpisany algorytmem SHA-256
- Dowolna nazwa domeny
- Certyfikat rozpoznawalny domyślnie na urządzeniach mobilnych

Pozyskanie certyfikatu (oraz jego instalacja) i domeny, dla której zostanie wystawiony leży w gestii Zakładu dealerskiego.

Zakład dealerski może wykorzystać w tym celu już posiadany certyfikat publiczny jeśli będzie on odpowiadał powyższym wymaganiom i przeznaczeniu.

Konfigurowana witryna będzie dostępna tylko w sieci LAN dla urządzeń mobilnych.

2.2.2 Serwer DNS

Do zrealizowania poprawnej komunikacji SSL w sieci dealera konieczny jest lokalny serwer DNS. Serwer powinien posiadać konfigurację, która umożliwi prawidłowe rozwiązanie adresu fqdn witryny (na adres IP w wewnętrznej sieci dealera) serwera IIS, która jest zabezpieczona certyfikatem SSL.

2.3 Niezbędne komponenty i licencje

Niezbędne komponenty i licencje:

- Microsoft IIS
- .NET Framework
- Licencja BMS
- Przeglądarka Chrome

Zgodnie z dokumentem ogólnych wymagań SoftVig.

2.4 Urządzenia i programy współpracujące

Programem współpracującym z aplikacją SvCloud jest DMS AutoStacja3. Wymagana jest aktualizacja DMS do wersji 1710_0317.

3 Wymagania techniczne systemu

3.1 Stacje klienckie

Stacje klienckie powinny spełniać wymagania techniczne systemu AutoStacja3.

3.2 Ekrany prezentacyjne

Zalecana rozdzielczość na ekranach telewizorów/monitorów to FullHD.

3.3 Urządzenia mobilne

Urządzeniami referencyjnymi są ***Samsung Galaxy Tab S2*** z systemem ***Android* (7.0)** oraz ***iPad mini 4*** z systemem ***iOS (aktualna wersja)***. Urządzenia te zapewniają właściwy komfort użytkowania oraz płynne działanie aplikacji. Ze względu na ilość dostępnych urządzeń na rynku, wskazujemy jedynie aspekty kluczowe przy wyborze.

Istotnymi parametrami konfiguracji, na które należy zwrócić uwagę w trakcie doboru sprzętu są:

- obsługa sieci WiFi 802.11
- rozdzielczość: 2048x1536 lub wyższa (dla takich rozdzielczości została zaprojektowana aplikacja)
- pamięć RAM: 3GB lub więcej
- przekątna: 8” lub większa
- aparat: 5Mpx lub więcej (zalecamy aparat z lampą błyskową - lepsza jakość zdjęć)

3.4 Serwer

Wymaganą konfigurację serwera wskazuje Tabela 1:

Aspekt	Opis
Zajętość dyskowa	Serwer IIS: ok. 100MB wolnego miejsca na dysku na dane witryny sieciowej.
Pozostałe zalecenia	Serwer dostępny w sieci LAN dla urządzeń współpracujących z systemem BMS.

Tabela 1

Zgodnie z dokumentem ogólnych wymagań SoftVig.

3.5 Sieć lokalna WiFi

Dedykowanym do pracy z Modułem blacharskim urządzeniem mobilnym jest tablet, w związku z czym w Zakładzie dealerskim wymagana będzie sieć bezprzewodowa.

- Za projekt, realizację budowy infrastruktury bezprzewodowej oraz jej utrzymanie odpowiedzialny jest Zakład dealerski.
- Zakład dealerski określa jakie ma być pokrycie sygnałem bezprzewodowym na terenie lokalizacji dealerskiej.
- Za konfigurację i zabezpieczenie infrastruktury sieci odpowiedzialny jest Zakład dealerski.

Rekomendujemy zastosowanie własnej polityki bezpieczeństwa w oparciu o poniższe zalecenia:

- Centralne zarządzanie punktami dostępowymi.
- Zastosowanie technologii pozwalającej na wykrywanie obcych punktów dostępowych „rogue AP". Obce AP powinny być usuwane.
- Blokowanie podłączenia się sieci typu Pear to Pear do sieci WLAN (sieci typu ad-hock).
- Użycie autentykacji stacji końcowych WLAN
  - Rekomendowane wdrożenie dwukierunkowej autentykacji zgodnie ze standardem 802.1x, autentykacja EAP-TLS (serwer Radius, CA)
  - Stosowanie dynamicznej wymiany kluczy per użytkownik i per sesja. Standard WPA2 z szyfracją symetryczną AES.
  - Zabezpieczenie sieci hasłem PSK. Hasła powinny posiadać minimum 16 znaków w tym cyfry, znaki specjalne, duże i małe litery. Zalecana jest częsta zmiana hasła na przykład w trybie tygodniowym.
- Centralne logowanie wszystkich prób autentykacji.
- Użycie komunikacje WLAN w standardzie WPA2 wykorzystującym silne szyfrowanie AES
- Dostęp administracyjny do konfiguracji urządzeń infrastruktury WLAN (kontrolerów, punktów dostępowych itp.) ograniczony do dedykowanego personelu IT i zabezpieczony silnymi hasłami (minimum 16 znaków w tym cyfry, znaki specjalne, duże i małe litery, częsta zmiana hasła na przykład w trybie miesięcznym).
- Infrastruktura WLAN oddzielna od innej infrastruktury WLAN Dealera na przykład sieci gościnnej.
- Utworzenie odrębnego segmentu sieci w warstwie L3 pozwalający na wdrożenie sieciowych elementów bezpieczeństwa, ACL itp.