



Instrukcja administratora



www.famoc.com

PUBLISHED BY

FAMOC S.A.

Ul. Wajdeloty 12A

80-437 Gdańsk

Copyright© 2008-2021 by Famoc S.A.

Wszystkie prawa zastrzeżone. Cała zawartość dokumentu stanowi wyłączną własność firmy Famoc S.A. i nie może być powielana ani dystrybuowana bez pisemnej zgody wydawcy. Publikacja może zawierać marki i nazwy produktów będące znakami towarowymi lub zarejestrowanymi znakami towarowymi poszczególnych właścicieli.

SPECYFIKACJE I INFORMACJE DOTYCZĄCE PRODUKTÓW I USŁUG PRZEDSTAWIANYCH W INSTRUKCJI PODLEGAJĄ ZMIANOM. WSZELKIE INFORMACJE I ZALECENIA ZAMIESZCZONE W DOKUMENCIE SĄ WŁAŚCIWE JEDNAKŻE WSZELKA ODPOWIEDZIALNOŚĆ ZA IMPLEMENTACJĘ I UŻYTKOWANIE PRODUKTÓW I USŁUG LEŻY PO STRONIE UŻYTKOWNIKÓW.



Spis treści

1. Informacje o tym przewodniku	7
2. Czym jest FAMOC?	7
2.1 Zarządzanie zasobami mobilnymi	7
2.2 Zdalne zarządzanie konfiguracjami	8
2.3 Zdalne zarządzanie aplikacjami	8
2.4 Zdalne zarządzanie bezpieczeństwem	8
2.5 Zdalny dostęp	8
3. Komponenty FAMOC	9
3.1 Serwer FAMOC	9
3.2 Aplikacje mobilne FAMOC	9
3.3 Agent bazowy	9
3.4 Backup agent	9
3.5 Zdalny dostęp	9
3.6 Monitor lokalizacji	9
3.7 Monitor użycia	10
4. Bezpieczeństwo	10
5. Wspierane mobilne systemy operacyjne	10
6. Konsola administratora	10
7. Użytkowanie FAMOC	11
8. Tworzenie nowych organizacji i kont administratorów	13
8.1 Organizacje	14
8.2 Administratorzy	14
8.3 Role	15
8.4 Niestandardowe pola	16
8.5 Tłumaczenia	16
8.6 Status serwera	17
9. Kreator FAMOC	17
10. Dodawanie nowych użytkowników	19
10.1 Dodawanie pojedynczego użytkownika	19
10.2 Import użytkowników	21
10.3 Synchronizacja danych z serwerem zewnętrznym	22
Global Catalog	24
11. Organizacja	24
11.1 Użytkownicy	24
11.2 Szczegóły organizacji	24
11.3 Moje dane	24
11.4 Grupy	24
11.4.1 Tworzenie nowej grupy	25

11.4.2 Import grup	26
11.5 Importy	26
11.5.1 Import z LDAP	26
11.5.2 Import z pliku	26
11.5.3 Import schematów	27
11.6 Słowniki	27
11.7 Role	27
12. Monitoring	28
13. Urządzenia	29
13.1 Dodawanie pojedynczego urządzenia	30
13.2 Dodawanie grupy urządzeń (import)	31
13.3 Zarządzanie pojedynczym urządzeniem	31
13.3.1 Szczegóły	32
13.3.2 Użytkownicy	32
13.3.3 Aplikacje	32
13.3.4 Polityki	33
13.3.5 Agenty	33
13.3.6 Alerty	34
13.3.7 Log	34
13.3.8 Lokalizacja	34
13.3.9 Bezpieczeństwo	34
13.3.10 Kopia zapasowa	35
Kopia zapasowa/odzyskiwanie danych	35
Import danych	35
13.3.11 Karty SIM	36
13.3.12 Monitor urządzenia	36
13.3.13 Naprawy	36
13.3.14 Dane użytkownika	36
13.3.15 Zarejestrowane połączenia	36
13.4 Instalowanie certyfikatów i agenta podstawowego na poszczególnych urządzeniach	36
14.Karty SIM	37
15.Centrum konfiguracji	39
15.1 Agenty	39
15.1.1 Instalacja certyfikatu	39
15.2 Aplikacje	40
15.2.1 Dodawanie aplikacji z Apple App Store	40
15.2.2 Dodawanie aplikacji z Google Play	41
15.2.3 Dodawanie aplikacji niestandardowych	41
15.2.4 Zarządzanie grupami aplikacji	42
15.2.5 Instalacja aplikacji na telefonie	42
15.3 Sklep firmowy	43
15.3.1 Dodawanie sklepu firmowego	43

15.4 Konfiguracje	43
15.4.1 Dodanie nowej konfiguracji	45
15.4.2 Wysyłanie konfiguracji na urządzenia zdalne	45
15.5 Wiadomości	45
15.6 Backup	46
16. Zdalny pulpit	47
16.1 Instalacja zdalnego dostępu	47
16.2 Uruchomienie sesji zdalnego dostępu	47
16.3 Panel zdalnego pulpitu	48
16.3.1 Monitor urządzenia	49
16.3.2 Menadżer plików	49
16.3.3 Konfiguracje	49
17. Log	49
18. Lokalizacja	50
19. Alerty	51
20. Ustawienia	52
20.1 Polityki	52
20.2 Alerty	53
20.2.1 Typy alertów	53
20.2.2 Przekierowanie alertów	53
20.2.3 Lista zabronionych aplikacji	55
21.2.4 Lista dozwolonych aplikacji	55
21.3 Serwery	56
21.4 Ustawienia zaawansowane	59
21.4.1 Startup	59
21.4.2 Niestandardowe pola	62
21.4.3 Typy konfiguracji	62
21.4.4 Polityki referencyjne	63
21.4.5 Certyfikat Apple	63
21.4.6 Ustawienia VPP	64
21.4.7 Ustawienia iOS DEP	65
21.4.8 Apple Configurator	67
22.4.9 Proxy do Exchange	67
21.4.10 Zewnętrzny kontroler zgodności.	68
21.4.11 Zarządzanie grupami aplikacji	69
21.4.12 Zarządzanie grupami urządzeń	69
21.4.13 Ustawienia Android Enterprise	70
21.4.14 Ustawienia Knox Mobile Enrollment	70
21.4.15 Samsung E-FOTA	71
22. Raporty	72
22.1 Raporty FAMOC	72
22.2 Możliwe operacje dostępne w zakładce Raporty	73

1. Informacje o tym przewodniku

Zapoznanie się z niniejszym przewodnikiem administratora pozwoli poznać główne komponenty i funkcje FAMOC i dowiedzieć się jak:

- FancyFon Mobility Center (FAMOC™) może Tobie pomóc;
- FAMOC będzie działać dla Twojej firmy, użytkowników końcowych lub Twoich klientów;
- tworzyć wiele oddzielnych organizacji/działów na serwerze FAMOC i przyznawać różne uprawnienia do zarządzania różnym administratorom systemu;
- dostosować konsolę FAMOC, np. poprzez dodawanie nowych tłumaczeń systemowych i pól niestandardowych, przygotowywanie operacji pakietowych odpowiadających konkretnym potrzebom firmy lub zmianę konfiguracji agenta FAMOC;
- dodawać pojedynczych użytkowników i urządzenia do FAMOC lub importować masowo za pomocą synchronizacji serwera lub importu plików i mapowania danych;
- zdalnie zarządzać urządzeniami użytkowników końcowych (instalowanie aplikacji, wykonywanie konfiguracji bezprzewodowych, inicjowanie tworzenia kopii zapasowych itp.);
- zyskać nadzór nad infrastrukturą mobilną, monitorować parametry urządzenia, natychmiastowo identyfikować awarie i rozwiązywać problemy z urządzeniami za pomocą panelu nawigacyjnego, wykazu urządzeń, dziennika, alertów i raportów;
- nawiązać połączenie z telefonem klienta za pomocą zdalnego dostępu FAMOC;
- używać Monitora lokalizacji, aby zlokalizować urządzenia i użytkowników;
- monitorować status serwera i licencje FAMOC;
- oraz gdzie szukać bardziej szczegółowych informacji i wsparcia.

2. Czym jest FAMOC?

FAMOC to kompleksowe rozwiązanie umożliwiające użytkownikom zdalne zarządzanie dowolną liczbą urządzeń mobilnych przez Internet. Administratorzy firmy, a także dostawcy usług mogą korzystać z FAMOC, aby zapewnić natychmiastowe zdalne wsparcie dla użytkowników końcowych i pracowników.

FAMOC zarządza dowolnym urządzeniem mobilnym z systemem operacyjnym Android, iOS, Windows Phone 8, Windows Mobile 5.x i 6.x lub nowszym, Symbian OS v9.x (zarówno platformy S60, jak i UIQ), urządzeniami BlackBerry zaczynającymi się od wersji 4.3 systemu operacyjnego, telefonami opartymi na technologii Java z odpowiednimi ulepszeniami Java Mobile Edition (patrz: Matryca funkcjonalności FAMOC).

FAMOC zapewnia kompleksowe zarządzanie cyklem życia urządzeń mobilnych i niespotykany poziom wsparcia w zakresie bezpieczeństwa. Funkcjonalność systemu podzielona jest na pięć głównych elementów:

2.1 Zarządzanie zasobami mobilnymi

FAMOC identyfikuje wszystkie zasoby w ramach infrastruktury mobilnej przedsiębiorstwa i przechowuje wszystkie zebrane dane, budując tym samym kompletną bazę informacji o zasobach firmy, w tym o sprzęcie, oprogramowaniu, kartach SIM, użytkownikach i przetwarzaniu informacji. FAMOC Asset Manager zapewnia

wgląd w czasie rzeczywistym w środowisko mobilne organizacji i jest niezwykle pomocne przy planowaniu przyszłych działań.

2.2 Zdalne zarządzanie konfiguracjami

FAMOC umożliwia administratorom wykonywanie wszelkich zadań związanych z konfigurowaniem konfiguracji bezprzewodowych i obsługuje szeroki zakres urządzeń i systemów operacyjnych. To rozwiązanie śledzi dane zarówno poszczególnych zasobów, jak i całego systemu (numer wersji i modelu, wydajność bazową, relacje z innymi zasobami), umożliwiając zdalną konfigurację parametrów i wdrażanie polityk korporacyjnych.

2.3 Zdalne zarządzanie aplikacjami

FAMOC automatycznie wykrywa i raportuje o flocie mobilnej przedsiębiorstwa, zapewniając wgląd w czasie rzeczywistym w status i użycie wszystkich aplikacji. Ponadto synchronizuje dane przechowywane na urządzeniach mobilnych w celu zapewnienia kopii zapasowych i dostępu do współdzielonych zasobów oraz umożliwia zdalną administrację i bezprzewodową synchronizację danych.

2.4 Zdalne zarządzanie bezpieczeństwem

FAMOC zapewnia niezrównany poziom wsparcia bezpieczeństwa na wielu platformach mobilnych, poprzez centralne, bezprzewodowe zarządzanie. To rozwiązanie zapewnia bezpieczną komunikację między serwerem a urządzeniami mobilnymi, chroniąc przechowywane dane i umożliwiając bezproblemowe wdrożenie polityki korporacyjnej.

2.5 Zdalny dostęp

FAMOC Remote Access to wysoce bezpieczne i łatwe w użyciu rozwiązanie, które umożliwia rozwiązywanie problemów z urządzeniami mobilnymi, pozwalając administratorowi na ich zdalne obsługiwanie poprzez połączenie sieciowe (np. GPRS / EDGE / 3G, WiFi), wyświetlając ekran urządzenia i dając dostęp do jego klawiatury bezprzewodowo.

Możliwości, które daje FAMOC to:

- Zdalna kontrola nad smartfonami
- Obniżone koszty wsparcia
- Zwiększona satysfakcja użytkownika
- Przyspieszone wdrażanie nowych usług
- Usprawnione rozwiązywanie problemów
- Sprawdzona technologia pomocy technicznej
- Rozwiązywanie trudnych problemów dla Twoich szczególnie cenionych klientów

3. Komponenty FAMOC

FAMOC składa się z kilku elementów, zaprojektowanych w taki sposób, aby efektywnie zarządzać dowolnej wielkości flotą mobilną w czasie pełnego cyklu życia urządzeń.

3.1 Serwer FAMOC

Kluczowym elementem systemu jest serwer FAMOC, odpowiadający za procesy inwentaryzacyjne, zarządzający komunikacją z urządzeniami zdalnymi oraz obsługujący sesje zdalnego dostępu uruchamiane z poziomu konsoli webowej. System może korzystać z kilku serwerów fizycznych, w zależności od konfiguracji, możliwy jest dodatkowy fail-over, load-balancing lub serwer bazodanowy. Więcej informacji można uzyskać pod adresem support@fancyfon.com.

3.2 Aplikacje mobilne FAMOC

Agenty (aplikacje mobilne) FAMOC instalowane są na urządzeniach zdalnych i bezpiecznie komunikują się z serwerem dostarczając wyczerpujących danych oraz umożliwiając szeroki zakres zarządzania. Poniżej znajdują się krótkie opisy poszczególnych rodzajów agentów.

3.3 Agent bazowy

Agent bazowy jest odpowiedzialny za zdalną instalację i usuwanie aplikacji, konfiguracji, zdalne czyszczenie danych oraz uruchamianie aplikacji, w tym także innych aplikacji klienckich FAMOC. Zapewnia również poprawną konfigurację restrikcji bezpieczeństwa i monitorowanie czy jest ona efektywnie egzekwowana. Wśród możliwych funkcji aplikacji jest m.in. blokowanie łączności Bluetooth, odebranie użytkownikowi możliwości instalacji aplikacji czy też wyłączenie dostępu do pewnych funkcji użytkowych telefonu. Dodatkowo umożliwia automatyczny pobór parametrów urządzenia m.in. adres Mac WLAN, uruchomione procesy, zainstalowane aplikacje i wiele innych.

3.4 Backup agent

Backup agent pozwala na przechowywanie kopii danych z urządzeń na centralnym serwerze FAMOC i łatwe odzyskiwanie danych w przypadku wymiany lub utraty urządzenia.

3.5 Zdalny dostęp

Zdalny dostęp pozwala administratorowi nawiązać połączenie z urządzeniem zdalnym i umożliwia zarządzanie klawiaturą i ekranem telefonu z poziomu platformy FAMOC. Aplikacja umożliwia przeglądanie plików zainstalowanych na telefonie, z poziomu konsoli administrator, podczas zdalnej sesji. Menedżer plików pozwala dodatkowo pobierać i wgrywać pliki i folder na urządzenie zdalne.

3.6 Monitor lokalizacji

Monitor lokalizacji pozwala śledzić i lokalizować zdalnie urządzenia mobilne.

3.7 Monitor użycia

Monitor użycia monitoruje i raportuje aktywność użytkownika do serwerów FAMOC.

4. Bezpieczeństwo

FAMOC zapewnia bezpieczeństwo przepływu danych w następujący sposób:

- Korzystając z systemu nie ma potrzeby otwierania dodatkowych portów na korporacyjnym lub osobistym firewallu, ponieważ komunikacja pomiędzy serwerem administratora a urządzeniem klienta odbywa się przy użyciu standardowego protokołu sieciowego (HTTPS). Funkcja Zdalnego Dostępu wymaga otwarcia jednego dodatkowego portu na firewallu – port ten jest konfigurowalny i można go dostosować do konkretnych potrzeb.
- System uzyskuje zakodowane połączenie pomiędzy administratorem i klientem przy użyciu standardowych protokołów internetowych (256-bit SSL).
- Sesja zdalnego dostępu musi być zaakceptowana przez użytkownika – administrator nie ma prawa dostępu do telefonu bez wcześniejszej zgody użytkownika.
- Sesje pomocy technicznej są inicjowane przez użytkownika – administrator nie ma prawa dostępu do telefonu bez zaproszenia do niego przez klienta lub bez wyraźnej zgody użytkownika.
- Niezwłocznie po zakończeniu sesji, wszelkie prawa dostępu do urządzenia klienta zostają usunięte.
- Wszystkie sesje są nagrywane, zwiększając bezpieczeństwo i uniemożliwiając nadużycia.

5. Wspierane mobilne systemy operacyjne

- Android (smartfony i tablety)
- Apple iPhone oraz iPad
- Apple tvOS, MacOS
- Microsoft Windows Phone 8 oraz Windows Phone 8.1
- Windows 10 Mobile
- Windows 8.1+

6. Konsola administratora

W konsoli administratora znajdują się takie funkcjonalności jak ustawienia bezpieczeństwa, uwierzytelnianie tożsamości użytkownika, komunikacja, logowanie oraz raportowanie.

1. Aby rozpocząć pracę z systemem FAMOC, należy zalogować się na stronie <https://<nazwa-serwera>>, używając loginu i hasła dostarczonego przez administratora.
2. Po zalogowaniu wyświetlany jest spis urządzeń bieżącej organizacji.

UWAGA: Przy pierwszym logowaniu wymagane jest zaakceptowanie „Umowy licencyjnej użytkownika końcowego”.

Umowa licencyjna użytkownika końcowego - FAMOC

Niniejsza umowa licencyjna użytkownika końcowego (zwana dalej „Umową”) jest umową pomiędzy Użytkownikiem (zwanym dalej „Użytkownikiem”) oraz firmą FancyFon S.A. (zwaną dalej „FancyFon”). W rozumieniu niniejszej umowy Użytkownik oznacza osobę fizyczną oraz spółkę, w imieniu której Użytkownik korzysta (lub ułatwia korzystanie) z Oprogramowania jako pracownik lub podmiot („Spółka”). Użytkownik reprezentuje i gwarantuje, że posiada uprawnienia, moc i możliwość przystąpienia do Umowy w imieniu Spółki, oraz że Umowa stanowi prawnie wiążący obowiązek Spółki, ciążyący na Spółce zgodnie z jej warunkami.

WYBIERAJĄC OPCJĘ „AKCEPTUJ”, INSTALUJĄC LUB UŻYWAJĄC OPROGRAMOWANIE, UŻYTKOWNIK POTWIERDZA, ŻE PRZECZYTAŁ NINIEJSZĄ UMOWĘ, RUZUMIE JEJ TREŚĆ I ZGADZA SIĘ PRZESTRZEGAĆ JEJ ZASAD I WARUNKÓW. JEŻELI UŻYTKOWNIK NIE AKCEPTUJE WARUNKÓW, NALEŻY WYBRAĆ OPCJĘ „ODMOWA” I ODINSTALOWAĆ OPROGRAMOWANIE. FIRMA FANCYFON MOŻE WPROWADZAĆ ZMIANY DO NINIEJSZEJ UMOWY PO UPRZEDNIM POINFORMOWANIU UŻYTKOWNIKA. ZGADZAJĄC SIĘ NA ZMODYFIKOWANE WARUNKI UMOWY LUB UŻYWAJĄC OPROGRAMOWANIA PO UPRZEDNIM POINFORMOWANIU O ZMIANACH, UŻYTKOWNIK WYRAŻA ZGODĘ NA WSZYSTKIE DOKONANE MODYFIKACJE.

1. DEFINICJE. „Urządzenie” oznacza urządzenie mobilne użytkownika. „Oprogramowanie” oznacza (i) oprogramowanie firmy FancyFon w formacie przeznaczonym do odczytu komputerowego udostępnione do użycia na Urządzeniu oraz (ii) dowolne aktualizacje oprogramowania. „Usługi online” oznaczają niektóre usługi, funkcjonalności i/lub funkcje będące dostępne Użytkownikowi podczas korzystania z Oprogramowania.

2. LICENCJA. FancyFon udziela Użytkownikowi niewyłącznej, nieprzenoszalnej licencji bez prawa udzielenia podlicencji do (i) instalacji i korzystania z Oprogramowania oraz (ii) korzystania z Usług online, oraz wykorzystania licencji odpowiednio dla liczby Urządzeń, dla których licencja została zakupiona, wyłącznie do wewnętrznego użytku służbowego na warunkach i zgodnie z niniejszą Umową.

3. RESTRYKCJE. Użytkownik zobowiązuje się nie: (i) powielać, modyfikować, tworzyć produktów pochodnych, dystrybuować, sublicencjonować, przekazywać Oprogramowania, (ii) korzystać z Oprogramowania, przynosząc korzyści

☐ Wyrażam zgodę na wszystkie warunki umowy licencyjnej FAMOC (EULA).*

Anuluj

Potwierdź

Rysunek 1 Umowa licencyjna użytkownika końcowego

Aby wejść do zaawansowanych ustawień FAMOC należy po zatwierdzeniu Licencji kliknąć zakładkę **ZAAWANSOWANE**.

Górne menu zawiera trzy podstawowe zakładki: **ZARZĄDZANIE**, **ZAAWANSOWANE** oraz **ORGANIZACJA**.

Zakładka **ORGANIZACJA** umożliwia m.in. zarządzanie użytkownikami, grupami oraz przyznawanie dostępu do poszczególnych funkcji systemu.

Zakładka **ZAAWANSOWANE** zapewnia dostęp do zaawansowanych funkcjonalności związanych z zarządzaniem urządzeniami mobilnymi.

Z kolei zakładka **ZARZĄDZANIE** prowadzi do nowego interfejsu.

7. Użytkowanie FAMOC

Poniżej znajduje się tabela opisująca wszystkie zakładki platformy FAMOC.

ORGANIZACJA	
Użytkownicy	Dodawanie i usuwanie użytkowników, przyznawanie im uprawnień dostępu do ORGANIZACJI oraz konsoli FAMOC
Szczegóły organizacji	Wprowadzanie i edycja danych zarządzanej organizacji
Moje dane	Edycja danych użytkownika, zmiana hasła dostępu do konsoli, zmiana wersji językowej

Grupy	Tworzenie dowolnej liczby grup pracowniczych, dodawanie użytkowników do istniejących grup (funkcja bardzo przydatna przy zarządzaniu dużą organizacją)
Importy	Import danych użytkowników oraz synchronizacja danych z serwerem Open LDAP lub Active Directory
Słowniki	Tworzenie dodatkowych słowników, umożliwiających bardziej szczegółowy opis zarządzanych telefonów lub kart SIM (funkcja przydatna przy korzystaniu z opcji zaawansowanego wyszukiwania)
Role	Tworzenie nowych ról użytkowników i nadawanie im określonych uprawnień do korzystania z systemu.

ZAAWANSOWANE

Monitoring*	Element nowego interfejsu. Personalizowane zestawienie alertów raportowanych do serwera FAMOC, status zarządzanych serwerów, ogólne dane o urządzeniach włączonych do usługi FAMOC
Urządzenia	Dodawanie pojedynczych oraz import grupy urządzeń, zestawienie danych o zarządzanych urządzeniach (np. IMEI, nr telefonu, producent urządzenia, karta SIM), Wykonywanie instalacji aplikacji FAMOC, koniecznych do zdalnego zarządzania flotą mobilną
Karty SIM	Lista kart SIM objętych usługą FAMOC
Centrum konfiguracji	Zarządzanie aplikacjami klienckimi FAMOC, profilami, aplikacjami trzecimi (w tym aplikacje klienta), konfiguracjami, operacjami, SMS-ami i pakietami instalacji agentów/aplikacji do jednoczesnego przeprowadzenia na grupie urządzeń. Opis poszczególnych zakładek znajduje się poniżej.
Zdalny pulpit	Uruchomienie sesji zdalnego dostępu i przejęcie kontroli nad ekranem i klawiaturą urządzenia zarejestrowanego w usłudze FAMOC
Log	Przegląd działań podjętych na wszystkich urządzeniach włączonych do usługi FAMOC
Lokalizacja	Śledzenie i lokalizowanie urządzeń mobilnych
Alerty	Wgląd w alerty raportowane do systemu. Alerty mogą być przekazywane wybranym użytkownikom drogą mailową lub przez sms
Ustawienia	Synchronizacja danych z serwerami zewnętrznymi, tworzenie niestandardowych pól w systemie, konfiguracja aplikacji klienckich FAMOC
Raporty	Generowanie raportów i statystyk o urządzeniach podłączonych do usługi FAMOC według harmonogramu lub na żądanie

ZARZĄDZANIE*

Monitoring	Konfigurowalne zestawienie raportów FAMOC, pokazujące aktualny status systemu, zawierający ogólne informacje o FAMOC oraz urządzeniach włączonych do usługi
Users	Nowa zakładka zarządzania użytkownikami
Devices	Nowa zakładka zarządzania urządzeniami
Applications	Nowa zakładka zarządzania aplikacjami
Advanced	Przekierowuje do Zakładki ZARZĄDZANIE w starym interfejsie

Tabela 1 Zakładki systemowe

*dodatkowe informacje o nowym interfejsie znajdują się w dokumencie: FAMOC UI Guide.

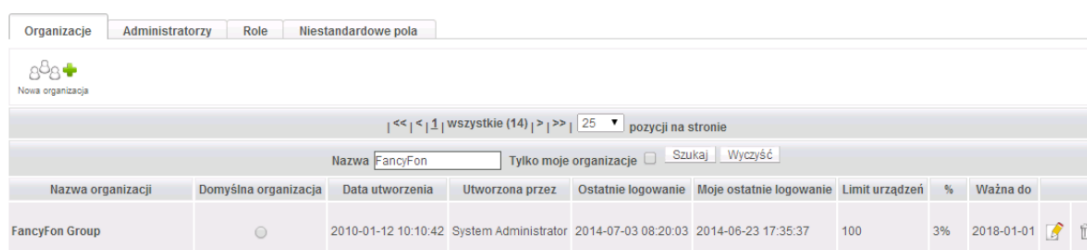
8. Tworzenie nowych organizacji i kont administratorów

Administrator ma możliwość dodawania, edytowania i usuwania organizacji i administratorów. Jeśli administrator systemu FAMOC posiada takie uprawnienia, to po zalogowaniu do systemu i użyciu przycisku

, wyświetlona zostanie lista poniższych zakładek zarządzania:

- Organizacje – pozwala dodawać nowe organizacje/departamenty FAMOC, czyli stworzyć na serwerze osobną przestrzeń/jednostkę, do której przypisani będą konkretni użytkownicy, administrator i odpowiednie pełnomocnictwa w zakresie zarządzania
- Administratorzy – pozwala nadać użytkownikom dostęp i pełnomocnictwa zarządzania dla nowo utworzonych organizacji
- Role – zakładka umożliwia dodawanie nowych ról administracyjnych (określonych zestawów pełnomocnictw)
- Niestandardowe pola – zakładka umożliwia dodanie dodatkowych pól dla organizacji
- Tłumaczenia – tutaj możliwe jest tworzenie nowych wersji językowych interfejsu FAMOC, tj. tłumaczenie zakładek oraz poleceń
- Status serwera – zakładka dostarcza wyczerpujących danych na temat statusu serwisów, licencji serwera i certyfikatów SSL

Jeżeli administrator otrzymał dostęp do wielu organizacji to ta zakładka pozwala na przełączanie się między nimi.



Nazwa organizacji	Domyślna organizacja	Data utworzenia	Utworzona przez	Ostatnie logowanie	Moje ostatnie logowanie	Limit urzędzeń	%	Ważna do	
FancyFon Group		2010-01-12 10:10:42	System Administrator	2014-07-03 08:20:03	2014-06-23 17:35:37	100	3%	2018-01-01	 

Rysunek 2 Zarządzanie organizacjami

8.1 Organizacje

1. Aby stworzyć nową organizację, użyj przycisku Nowa organizacja
2. Zdefiniuj nazwę organizacji/jednostki, wprowadź niezbędne dane, a następnie określ jak duże uprawnienia uzyska administrator nowej organizacji. FAMOC oferuje kilka szablonowych zestawów uprawnień:

- Administrator systemu FAMOC – dostęp do pełnej funkcjonalności systemu FAMOC
- Menedżer bezpieczeństwa FAMOC – dostęp do funkcji związanych z zarządzaniem bezpieczeństwem w organizacji

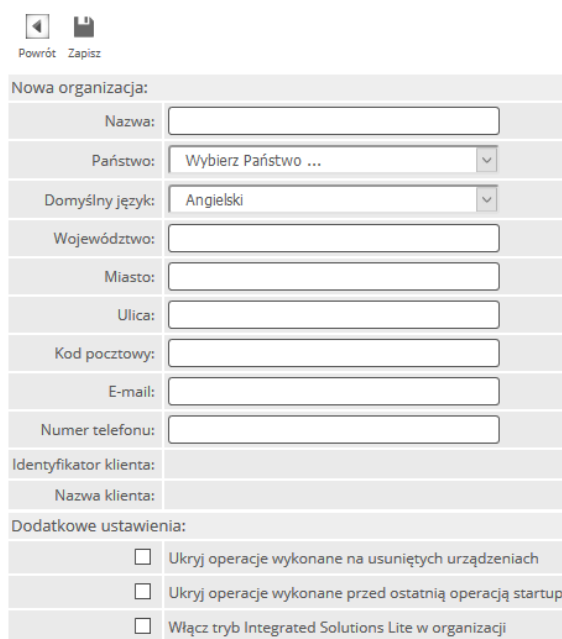
- Menedżer zasobów FAMOC – dostęp do informacji o zasobach mobilnych (hardware i software urządzeń, dane o kartach SIM, dane użytkowników końcowych itd.)
- Menedżer grup FAMOC – dostęp do zakładki umożliwiającej zarządzanie grup użytkowników i urządzeń
- FAMOC Web Services – dostęp do usług web-serwisowych

3. Dodatkowe ustawienia dla organizacji:

- Ukryj operacje wykonane na usuniętych urządzeniach – ukrywa wpisy usuniętych urządzeń w zakładce logów;
- Ukryj operacje wykonane przed ostatnią operacją startup – ukrywa wpisy w zakładce logów dla operacji wykonanych przed ostatnią rejestracją;
- Włącz tryb FAMOC Lite w organizacji – aby dowiedzieć się więcej o FAMOC Lite, zapoznaj się z dokumentem „FAMOC Lite”.

4. Następnie przypisz administratora do nowo utworzonej organizacji. Wystarczy podać login użytkownika oraz nadać mu tymczasowe hasło w zakładce Administrator organizacji. Hasło należy zmienić po pierwszym logowaniu do systemu.

5. Zakończenie procesu wymaga wciśnięcia przycisku Zapisz.



Powrót Zapisz

Nowa organizacja:

Nazwa:

Państwo:

Domyślny język:

Województwo:

Miasto:

Ulica:

Kod pocztowy:

E-mail:

Numer telefonu:

Identyfikator klienta:

Nazwa klienta:

Dodatkowe ustawienia:

☐ Ukryj operacje wykonane na usuniętych urządzeniach

☐ Ukryj operacje wykonane przed ostatnią operacją startup

☐ Włącz tryb Integrated Solutions Lite w organizacji

Rysunek 3 Tworzenie organizacji

8.2 Administratorzy

Zakładka Administratorzy pozwala dodawać nowych użytkowników o uprawnieniach administracyjnych oraz daje wgląd w takie dane jak login, imię, nazwisko, domyślna organizacja i lista organizacji, do których mają dostęp. Dodatkowo, ta sekcja pozwala na dodawanie dodatkowych funkcji zarządzających, rozszerzenie lub zmniejszenie uprawnień o kolejną organizację lub usunięcie użytkownika.

- Tabela: organizacja albo licencja
- Typ: tekst, liczba, data, hasło

Aby dodać niestandardowe pole:

1. Naciśnij Dodaj niestandardowe pole w zakładce Niestandardowe pola.
2. Uzupełnij pole Nazwa niestandardowego pola.
3. Wybierz Tabele i Typ.
4. Aby zakończyć zapisz ustawienia.

Name	Type	Table		
Custom field date	Text	Organizations		
Licence CF	Password	License		

Rysunek 6 Zakładka niestandardowe pola

8.5 Tłumaczenia

FAMOC oferuje kilka wersji językowych interfejsu¹ i umożliwia tworzenie dodatkowych tłumaczeń konsoli. Zakładka Tłumaczenia jest dostępna dla ról semi-administratora, administratora i superadministratora.

Aby utworzyć nową wersję językową konsoli:

1. Wejdź w zakładkę **Tłumaczenia** → **Języki**.
2. Wprowadź nazwę Języka i naciśnij **Zapisz** w celu utworzenia nowej zakładki pod tłumaczenie.
3. Otwórz nowo utworzoną zakładkę i uzupełnij tłumaczenia wylistowanych zagadnień, za każdym razem klikając OK w celu zapisania tłumaczenia do słownika.

Zaznaczenie opcji Aktywny obok danej wersji językowej w zakładce Języki spowoduje dodanie jej do opcji widocznych w każdej organizacji FAMOC.

¹ FAMOC oferuje obecnie polską, angielską i niemiecką wersję językową.

Języki	Angielski								
Język	Stan	Status tłumaczenia	Przypisane organizacje	Przypisani użytkownicy	Ostatnia zmiana	Import	Akcje		
Angielski (Domyślny język)	✓	100%	1	12	2019-12-05 12:04:03				
Polski	✓	99.99%	3	16	2019-12-05 12:04:03				
Niemiecki	✓	7.94%	0	0					
Angielski	✓	0%	0	0		Przeładaj...	Nie wybrano pliku.	Eksport	Wyłącz
	✗								
	✗								
	✗								
	✗								
	✗								
	✗								
	✗								
	✗								
	✗								
	✗								

Zapisz

Rysunek 7 Tłumaczenia

8.6 Status serwera

W tej sekcji znajdują się następujące zakładki:

- Status serwisów – w tej sekcji znaleźć można wyczerpujące dane na temat status usług świadczonych w ramach systemu FAMOC.
- Licencje serwera – zakładka udostępnia dane o limitach licencyjnych (maksymalnej liczbie urządzeń, którymi można zarządzać) oraz terminie wygaśnięcia licencji.
- Raporty – zakładka zawiera listę raportów serwera (w tym raporty licencyjne, które rejestrują organizacje utworzone przez superadministrатора wraz z numerami urządzeń zarządzanych w ramach działu oraz limitów licencji).

Administrator może dzięki tej sekcji generować raporty o licencjach dla każdej instytucji. Administrator może wyświetlić szczegółowe informacje na temat np. aktywnych urządzeń w każdej organizacji, liczbie wysłanych wiadomości tekstowych i SMS-ów binarnych, powiadomieniach push dla iOS i Android oraz pobrać raport jako plik tekstowy, .csv lub plik binarny, oraz zaplanować harmonogram raportów, które będą wysyłane jako e-mail.

generowanie raportów o instytucjach / organizacjach zarządzanych w systemie FAMOC wraz ze szczegółowymi danymi dotyczącymi liczby obsługiwanych w tych organizacjach urządzeń zdalnych. Raporty obejmują okresy miesięczne – żądany miesiąc wybierany jest w polu „Wybierz miesiąc:”. System umożliwia eksport danych do pliku (.txt, .csv oddzielone przecinkami lub .csv oddzielone średnikami) lub przesłanie raportu bezpośrednio na wskazany adres mailowy.

- Certyfikaty SSL – zawiera szczegóły dotyczące wykorzystywanych certyfikatów SSL

Status serwisów	Licencje serwera	Raporty	Certyfikaty SSL
Uruchom usługi	Zatrzymaj usługi	Uruchom ponownie usługi	

Status usług FancyFon					Odśwież
Nazwa programu	Szczegóły		Opis	Status	Status licencji
FAMOC Proxy	działa	OK	Proxy server	OK	-
	localhost	OK			
	localhost:11030	OK			
Remote Access	działa	OK	Remote Access server	OK	Pokryte
	localhost:11010	OK			
	localhost:11012	OK			
	localhost:11023	OK			
	/var/drad.http	OK			
	/var/dmd-drad	OK			
	/var/rda	OK			
Device Monitor	działa	OK	Device Monitor server	OK	Pokryte
	localhost:11014	OK			
	localhost:11015	OK			
	/var/rda-param	OK			

Rysunek 8 Status serwera

9. Kreator FAMOC

Po zalogowaniu do systemu (jeśli kroki kreatora nie zostaną wykonane) na ekranie pojawi się okienko pop-up prezentujące wszystkie dostępne kroki kreatora. Dodatkowo, lista ta może zostać wyświetlona po kliknięciu przycisku Kreator FAMOC, w prawym górnym rogu konsoli.

Kreator					×
Kroki kreatora			Status		
Dodanie użytkowników i grup			✓	ukryj	
Dodanie pojedynczego użytkownika			✓		
Konfiguracja LDAP/AD			✗	kontynuuj	pomiń
Import użytkowników i grup z pliku			✓		
Dodanie grupy użytkowników			✓		
Konfiguracja systemu			✓	ukryj	
Instalacja certyfikatu Apple APNS			✓		
Dodanie urządzeń do systemu			✓	ukryj	
Dodanie pojedynczego urządzenia			✓		
Dodanie urządzenia do systemu przez stronę startową			✓		
Zdefiniowanie polityk urządzeń mobilnych			✓	ukryj	
Zdefiniowanie polityk dla grup użytkowników lub grup urządzeń			✓		

Pokaż nie zrobione kroki

Zamknij

Rysunek 9 Kreator FAMOC

Pełna lista kroków kreatora FAMOC:

- Dodanie użytkowników i grup – oferuje kilka sposobów dodania nowych użytkowników i grup do systemu. Ten krok nie będzie pokazany w kreatorze, jeśli w systemie jest więcej niż jeden użytkownik i grupa. Administrator ma możliwość wybrania jednej z następujących opcji kreatora:
- Dodanie pojedynczego użytkownika – przycisk Kontynuuj kieruje do formularza w zakładce **ORGANIZACJA** → **Użytkownicy** → **Dodaj użytkownika**
- Konfiguracja LDAP/AD – przycisk Kontynuuj otwiera zakładkę **ORGANIZACJA**
- Importy → Import z LDAP - Import użytkowników i grup z pliku – przycisk Kontynuuj otwiera zakładkę **ORGANIZACJA** → **Importy** → **Import z pliku**
- Dodanie grupy użytkowników – przycisk Kontynuuj kieruje do formularza w zakładce **ORGANIZACJA** → **Grupy** → **Dodaj grupę**
- Konfiguracja systemu – zarządzanie urządzeniami iOS wymaga uprzedniego wgrania certyfikatu Apple APNS. Kreator kieruje do odpowiedniego formularza w systemie. Ten krok nie będzie widoczny, jeśli certyfikat został już wgrany na serwer FAMOC.
- Dodanie urządzeń do systemu – FAMOC udostępnia kilka sposobów dodawania urządzeń do system:
- Dodanie pojedynczego urządzenia – przycisk Kontynuuj kieruje do formularza w zakładce **ZAAWANSOWANE** → **Urządzenia** → **Dodaj urządzenie**
- Dodanie urządzeń do system przez stronę startową – przycisk Kontynuuj kieruje do zakładki **ZAAWANSOWANE** → **Ustawienia** → **Ustawienia zaawansowane** → **Startup**, w której widoczny jest link do strony startowej
- Definiowanie polityk urządzeń mobilnych – udostępnia odnośniki do formularzy umożliwiających definiowanie polityk podstawowych i polityk bezpieczeństwa dla grup użytkowników. FAMOC udostępnia następujące sposoby:
- Definiowanie polityk dla grup użytkowników – przycisk Kontynuuj kieruje do formularza w zakładce **ZAAWANSOWANE** → **Ustawienia** → **Polityki** → **Polityki podstawowe**
- Definiowanie polityk bezpieczeństwa dla grup użytkowników – przycisk Kontynuuj kieruje do formularza w zakładce **ZAAWANSOWANE** → **Ustawienia** → **Polityki** → **Polityki bezpieczeństwa**

W dolnej części okna kreatora, dostępne są dwa przyciski:

- Pokaż wszystkie kroki – wyświetla wszystkie kroki kreatora wraz ze statusem (wykonany, oczekujący, pominięty)
- Zamknij – zamyka popup

10. Dodawanie nowych użytkowników

Platforma FAMOC oferuje administratorowi możliwość dodawania pojedynczych użytkowników do systemu oraz opcję importu dowolnej liczby grup użytkowników poprzez załadowanie odpowiednio przygotowanego pliku lub poprzez synchronizację z serwerem Open LDAP lub Active Directory. Użytkownicy mogą być także automatycznie dodani do system poprzez synchronizację danych z serwerem BlackBerry Enterprise.²

² Więcej informacji na temat dodawania i synchronizacji serwerów RIM BlackBerry Enterprise Servers (BES 4.x, BES 5.x) znaleźć można w instrukcji BesAdapter for FAMOC Installation Guide.

10.1 Dodawanie pojedynczego użytkownika

1. Aby dodać nowego użytkownika, należy wybrać przycisk Dodaj użytkownika w zakładce

ZAAWANSOWANE → Urządzenia lub ORGANIZACJA → Użytkownicy.

2. Przy dodawaniu nowego użytkownika należy podać jego dane osobowe oraz przyporządkować mu Login. W tej zakładce można również zdefiniować ustawienia dostępu WLAN oraz dane pracownika. Administrator może opcjonalnie dodać nowego użytkownika do utworzonej wcześniej grupy. Zatwierdzenie wprowadzonych danych nastąpi po użyciu przycisku Zapisz.

Szczegóły użytkownika	Grupy	Role	Dostęp WLAN	Ustawienia APN	Aplikacje	Certyfikaty	Własne pola
Państwo:	Polska						
Firma:							
Dział:							
Stanowisko:							
Telefon do biura:							
Telefon komórkowy:							
Identyfikator:							
Email:							
Adres email							
Email - nazwa użytkownika							
Powrót Zapisz							

Rysunek 10 Dodawanie nowego użytkownika (1)

3. W przypadku, gdy administrator zamierza upoważnić danego użytkownika do logowania się do zakładki ORGANIZACJA oraz ZAAWANSOWANE administrator musi najpierw zdefiniować zestawy uprawnień do funkcji zarządzania FAMOC w zakładce ORGANIZACJA → Role (patrz 12.7). Role będą dostępne do wyboru, po zaznaczeniu pola wyboru **Może się logować**.

4. Kiedy pole **Może się logować** jest zaznaczone, możliwe jest także włączenie funkcji **Wymuś zmianę hasła przy najbliższym zalogowaniu**. Wymusza ona na użytkowniku zmianę hasła.

Nowy użytkownik:	
Imię:	
Nazwisko:	
Login:	
Może się logować	☐

Rysunek 11 Ustawienia hasła użytkownika

5. Aby wprowadzić parametry dla aplikacji Instant Messenger, IBM Lotus Notes Traveler, Microsoft Exchange czy Agito RoamAnywhere, należy udać się do zakładki Aplikacje.

Szczegóły użytkownika	Grupy	Role	Dostęp WLAN	Ustawienia APN	Aplikacje	Certyfikaty	Własne pola
Instant Messenger:							
IM - nazwa użytkownika							
Lotus Notes:							
Identyfikator użytkownika:							
Microsoft Exchange:							
Nazwa użytkownika:							
Adres e-mail:							
Domena:							
Hasło:							
ShoreTel RoamAnywhere:							
Nazwa użytkownika:							
Hasło:							
Directory Number:							
Enterprise Number:							
VPN:							
Nazwa użytkownika VPN:							
VPN Hasło:							
Powrót		Zapisz					

Rysunek 12 Zakładka Aplikacje

6. FAMOC umożliwia przypisanie użytkownikowi unikalnego certyfikatu. Odpowiedni plik pem/der lub pkcs#12 można załadować w zakładce Certyfikaty. Dodatkowo, administrator może określić wydawcę certyfikatu oraz daty ważności (przy użyciu pliku pem/der, wartości te zostaną uzupełnione automatycznie). Po zapisaniu zmian, ikona certyfikatu pojawi się w zakładce Użytkownicy. Ikona przedstawia szczegóły certyfikatu. Certyfikat może być wykorzystywany przy wysyłaniu takich konfiguracji jak WiFi czy autoryzacja APN.

UWAGA: FAMOC nie zapewnia weryfikacji certyfikatu. Upewnienie się, co do prawidłowości załadowanego pliku, leży po stronie administratora.

7. Zakładka Użytkownicy umożliwia także edycję danych oraz usunięcie użytkownika.

UWAGA: W przypadku, gdy serwer FAMOC jest zsynchronizowany z serwerem BlackBerry Enterprise Server (patrz 11.3) przycisk **Dodaj użytkownika** pojawia się w zakładce ZAAWANSOWANE → Urządzenia (patrz 13). Po kliknięciu otwiera on okienko pop-up. Wybranie opcji dodania użytkownika do serwera FAMOC oraz dodania użytkownika do serwera BES powoduje przeniesienie do odpowiedniej zakładki.

10.2 Import użytkowników

W celu przeprowadzenia grupowego importu użytkowników, użyj przycisku **Importuj użytkowników** w zakładce **ORGANIZACJA** → **Użytkownicy**.

Zostaniesz poproszony o wprowadzenie opisu/nazwy importu, określenie typu i formatu importu (parametry oddzielone przecinkiem, średnikiem, dwukropkiem czy tabulatorem), a następnie o wgranie przygotowanego uprzednio pliku.

Jeśli schemat mapowania parametrów został wcześniej wprowadzony do systemu, będzie on dostępny do wyboru podczas importowania pliku. W przeciwnym razie wybierz opcję Utwórz nowy schemat. Aby kontynuować, a następnie użyć przycisku Dalej.

Kolejnym krokiem jest przygotowanie schematu mapowania danych, czyli przypisanie parametrów zawartych w importowanym pliku do odpowiednich pól w systemie FAMOC. Poza mapowaniem parametrów, należy pamiętać o podaniu nazwy schematu.

UWAGA: Prawidłowe przeprowadzenie importu i mapowania wymaga uwzględnienia wśród parametrów loginu użytkowników.

Rysunek 13 Import użytkowników

Kliknij **Zapisz**, aby zachować schemat mapowania. Po Zapisaniu danych, na ekranie pojawi się podsumowanie przeprowadzanego importu uwzględniające dane importu oraz importowane rekordy. Możliwe będą następujące opcje:

- Powrót – spowoduje zapisanie przygotowanego schematu, późniejszy import i mapowanie danych z przygotowanego pliku będzie dostępne w zakładce **ORGANIZACJA** → **Importy** → **Import z pliku**
- Importuj – skutkuje automatycznym importem i mapowaniem parametrów zgodnie z przygotowanym schematem
- Sprawdź dane – umożliwia walidację danych przed przeprowadzeniem importu
- Usuń – wybór przycisku spowoduje usunięcie schematu importu

UWAGA: W przypadku, gdy wprowadzone dane nie okażą się poprawne, cały proces importowania danych trzeba będzie powtórzyć w prawidłowym formacie pliku.

Zaimportowany plik oraz schemat mapowania dostępny jest w zakładce **ORGANIZACJA** → **Importy** (patrz 12.5).

10.3 Synchronizacja danych z serwerem zewnętrznym

1. System FAMOC może być w prosty sposób zsynchronizowany z serwerami Open LDAP lub Active Directory. Proces ten zostanie rozpoczęty poprzez użycie przycisku Nowy serwer Open LDAP lub Nowy serwer Active Directory w zakładce **ORGANIZACJA** → **Importy** → **Import z LDAP**.

2. Kolejnym krokiem jest uzupełnienie niezbędnych danych

- Dane połączenia – w tej części znajdują się parametry konieczne do nawiązania połączenia z serwerem zewnętrznym m.in. typ i nazwa serwera, interwał połączenia, adres czy port.

Platforma FAMOC udostępnia opcję uwierzytelniania użytkowników poprzez serwer LDAP, co oznacza możliwość logowania do systemu FAMOC przy użyciu hasła do serwera firmowego.

Możesz wybrać **Przypisanie grupy użytkowników na podstawie atrybutu LDAP**, aby automatycznie przypisywać użytkowników do określonych grup, gdy wartość tego pola zostanie ustawiona w synchronizacji. Administrator może wybrać nazwę klasy LDAP i nazwę atrybutu. Następnie wybierz grupę, do której użytkownicy powinni zostać przypisani.

FAMOC generuje kody startup dla importowanych urządzeń. Można ustalić metodę dostarczenia kodu dla importowanych urządzeń: Auto, Email, SMS, Bez powiadomienia.

- **Mapowanie** – sekcja mapowania pozwala określić, które atrybuty dostępne na serwerze LDAP/Active Directory mają być przypisane do odpowiednich atrybutów na serwerze FAMOC. Przycisk Assign wyświetla drzewo zależności danych.
- **Mapowanie grup** – w tej zakładce administrator ma możliwość przypisania użytkowników do grup utworzonych poprzednio na serwerze LDAP/Active Directory i przeniesienia ich automatycznie na serwer FAMOC.
- **Mapowanie urządzeń** – pozwala na import urządzeń z LDAP/Active Directory do systemu FAMOC

3. Na koniec należy użyć przycisku Zapisz i przetestuj ustawienia lub Zapisz i zsynchronizuj.

Rysunek 14 Synchronizacja z serwerem zewnętrznym

Global Catalog

Usługa ta jest dostępna po porcie 3268. W ustawieniach importu LDAP powinien być użyty jako port połączenia oraz otwarty na systemowym firewallu.

Pole Położenie listy klas w drzewie powinno pozostać puste. Filtr musi zawierać informacje o grupie użytkowników np. 'memberof=CN=Global_group,CN=Users,DC=exchange,DC=com'.

11. Organizacja

Zakładka ORGANIZACJA umożliwia edycję danych dotyczących zarządzanej organizacji lub użytkowników końcowych, ustawienie wersji językowej interfejsu, tworzenie grup użytkowników, tworzenie dodatkowych opisów w systemie, zarządzanie uprawnieniami (dostępem do poszczególnych zakładek i opcji systemu) oraz zarządzanie importem danych do systemu.

11.1 Użytkownicy

Zakładka Użytkownicy wyświetla pełną listę użytkowników system FAMOC i umożliwia administratorowi edycję danych oraz przydzielanie odpowiednich uprawnień dostępu do zakładek ORGANIZACJA i ZAAWANSOWANE. Dodatkowo, zakładka pozwala na dodawanie nowych użytkowników do systemu i usuwanie ich oraz masowy import danych. Aby edytować informacje szczegółowe o użytkownikach należy użyć przycisku edytuj na wybranym użytkowniku.

11.2 Szczegóły organizacji

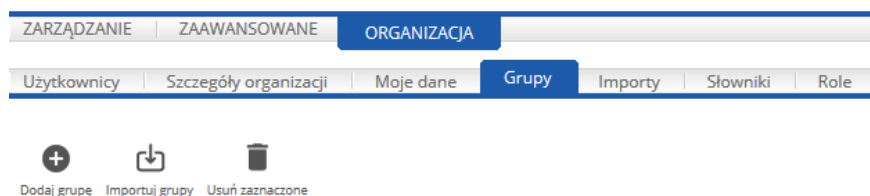
Zakładka Szczegóły organizacji pozwala edytować takie dane jak nazwa czy adres zarządzanej instytucji. Po wprowadzeniu zmian zatwierdź przyciskiem Zapisz.

11.3 Moje dane

Zakładka Moje dane pozwala przede wszystkim na edycję danych użytkownika, zmianę hasła oraz ustawienie wersji językowej interfejsu.

11.4 Grupy

Zakładka Grupy jest bardzo przydatna przy zarządzaniu dużą liczbą urządzeń i użytkowników ponieważ umożliwia grupowanie użytkowników według podobnych wymagań oraz przeprowadzenie działań na całej grupie.



Rysunek 15 Grupy

11.4.1 Tworzenie nowej grupy

1. Stworzenie nowej grupy użytkowników wymaga użycia przycisku Dodaj grupę w zakładce **ORGANIZACJA** → **Grupy**.

2. Wprowadź Nazwę grupy. Nazwa powinna być bezpośrednio powiązana z funkcjami grupy, takimi jak: pracownicy w Londynie, pracownicy działu sprzedaży itp. Dzięki temu praca administratora będzie bardziej wydajna. Można również zdefiniować warunki SLA (Service Level Agreement). System udostępnia cztery szablony SLA: Basic, Gold, Platinum lub VIP, dla różnych priorytetów wsparcia. Po zdefiniowaniu SLA w wykazie urządzeń pojawią się następujące ikony, które umożliwiają sortowanie urządzeń zgodnie z poziomem wsparcia:

- Podstawowy (Basic Service Level Agreement)
- Złoty (Gold Service Level Agreement)
- Platynowy (Platinum Service Level Agreement)
- V.I.P. (VIP Service Level Agreement)

W zakładce Pracownicy, wybierz użytkowników przypisanych do grupy i kliknij Zapisz.

Dodatkowo należy ustalić poziom kompetencji danej grupy. Zakładka Role pozwoli określić zakres dostępu do funkcjonalności systemu FAMOC. System oferuje kilka podstawowych zestawów kompetencji, natomiast elastyczne tworzenie ról systemowych możliwe jest w zakładce ORGANIZACJA → Role (patrz 12.7).

Nowa grupa została utworzona i jest wyświetlana na karcie Grupy. Grupy można modyfikować i usuwać z FAMOC, naciskając odpowiednie przyciski.

Rysunek 16 Tworzenie nowej grupy

11.4.2 Import grup

Aby wykonać zbiorczy import grup, należy użyć przycisku Importuj grupy w zakładce ORGANIZACJA → Grupy. Import pliku wymaga nadania nazwy, opisu oraz zdefiniowania formatu.

Import plików wymaga dodania opisu, wybrania formatu pliku oraz pliku do przesłania. Jeśli wcześniej utworzono schemat mapowania parametrów, będzie on dostępny do wyboru podczas importowania pliku. W przeciwnym razie wybierz opcję Utwórz nowy schemat. Cały proces jest analogiczny do opisywanego wcześniej importu użytkowników.

11.5 Importy

W zakładce Importy, administrator może dokonywać masowego importu użytkowników, grup, kart SIM, urzędzeń lub rachunków.

11.5.1 Import z LDAP

Sekcja umożliwia synchronizację serwera FAMOC z zewnętrznymi serwerami Open LDAP lub Active Directory. Więcej informacji na ten temat znaleźć można w rozdziale 11.3.

11.5.2 Import z pliku

W tej zakładce przechowywane są wszystkie załadowane do systemu pliki importu. Administrator ma możliwość sprawdzenia danych, zaimportowania ich, w przypadku, gdy etap ten został odłożony na później lub usunięcia pliku. Możliwe jest ponadto zainicjowanie nowego importu.

1. Aby rozpocząć Import nowego pliku kliknij przycisk Nowy import.
2. Wprowadź opis importu, wybierz typ i format importu (parametry oddzielone przecinkiem, średnikiem, dwukropkiem czy tabulatorem).
3. Następnie załaduj przygotowany uprzednio plik.
4. Jeśli schemat mapowania został wcześniej wprowadzony do systemu, będzie on dostępny podczas importowania pliku. W przeciwnym wypadku przy parametrze Schemat, należy wybrać opcję Utwórz nowy schemat, a następnie użyć przycisku Dalej.
5. Kolejnym krokiem jest przygotowanie schematu mapowania danych, czyli przypisanie parametrów zawartych w importowanym pliku do odpowiednich pól w systemie FAMOC. Poza mapowaniem parametrów, należy pamiętać o podaniu nazwy schematu.

UWAGA: Prawidłowe przeprowadzenie importu i mapowania wymaga uwzględnienia wśród parametrów loginu użytkowników.

6. Po Zapisaniu danych wgrany plik zostanie zweryfikowany pod kątem poprawności. Jeśli format pliku będzie poprawny zmieni on status na Zweryfikowany, a na liście pojawi się ikona importu . Po jej kliknięciu nastąpi automatyczny import i mapowanie parametrów zgodnie z przygotowanym schematem.

UWAGA: W przypadku, gdy wprowadzone dane nie okażą się poprawne (ikona ) , cały proces importowania danych trzeba będzie powtórzyć z prawidłowym formatem pliku.

7. Zarówno załadowane jak i zaimportowane pliki dostępne są w zakładce **ORGANIZACJA** → **Importy** → **Import z pliku**.

8. Aby usunąć schemat importu kliknij ikonę .

11.5.3 Import schematów

W tej sekcji znajduje się lista uprzednio przygotowanych schematów mapowania danych. Administrator ma możliwość przeglądania danych, usuwania schematów lub tworzenia nowych szablonów.

1. Aby utworzyć nowy schemat importu, należy użyć przycisku **Nowy schemat**.

2. Wprowadź opis importu, wybierz typ i format importu (parametry oddzielone przecinkiem, średnikiem, dwukropkiem czy tabulatorem) a następnie załaduj przygotowany uprzednio plik.

3. Kolejnym krokiem jest zdefiniowanie typu importu. Aby kontynuować należy wcisnąć przycisk Dalej.

4. Dodaj nazwę schematu mapowania oraz sparuj atrybuty załadowanego pliku z odpowiednimi polami w systemie FAMOC.

UWAGA: Prawidłowe przeprowadzenie importu i mapowania wymaga uwzględnienia wśród parametrów loginu użytkowników.

5. Zatwierdź ustawienia używając przycisku **Zapisz**.

11.6 Słowniki

Dodanie nowych słowników do systemu FAMOC umożliwia tworzenie bardziej szczegółowych i spersonalizowanych opisów urządzeń włączonych do usługi. Funkcja ta jest przydatna przy korzystaniu z opcji zaawansowanego wyszukiwania.

1. Aby dodać nowy słownik, użyj przycisku **Dodaj słownik**.

2. Wpisz Nazwę i Opis słownika.

3. Wpisz nowe słowa i Dodaj je do słownika.

5. Opcjonalnie do każdego słowa można dodać opis.

4. Zapisz ustawienia.

UWAGA: Zakładka Słowniki umożliwia dodawanie nowych kategorii opisowych do systemu. Jednak ich wykorzystanie przy opisie urządzeń, wymaga dodatkowo utworzenia tzn. Pól niestandardowych (patrz 21.4.2).

11.7 Role

W tej zakładce administrator tworzy szablony ról ze wstępnie zdefiniowanymi uprawnieniami użytkownika, które następnie będzie można przyznać nowym użytkownikom dodawanym do systemu. Dzięki temu nie będzie konieczne za każdym razem ręczne przydzielanie uprawnień.

FAMOC oferuje kilka szablonych ról systemowych:

- Administrator systemu FAMOC – dostęp do pełnej funkcjonalności systemu FAMOC
- Menedżer bezpieczeństwa FAMOC – dostęp do funkcji związanych z zarządzaniem bezpieczeństwem w organizacji
- Menedżer zasobów FAMOC – dostęp do informacji o zasobach mobilnych (hardware i software urządzeń, dane o kartach SIM, dane użytkowników końcowych itd.)
- Monitor Lokalizacji FAMOC – dostęp do zakładki umożliwiającej lokalizowanie urządzeń
- FAMOC Web Services – dostęp do usług web-serwisowych

Aby utworzyć nowy zestaw kompetencji, należy:

1. Użyć przycisku **Dodaj rolę** w zakładce **ORGANIZACJA** → **Role**.

2. Określić **Nazwę** i **Opis** nowej roli.

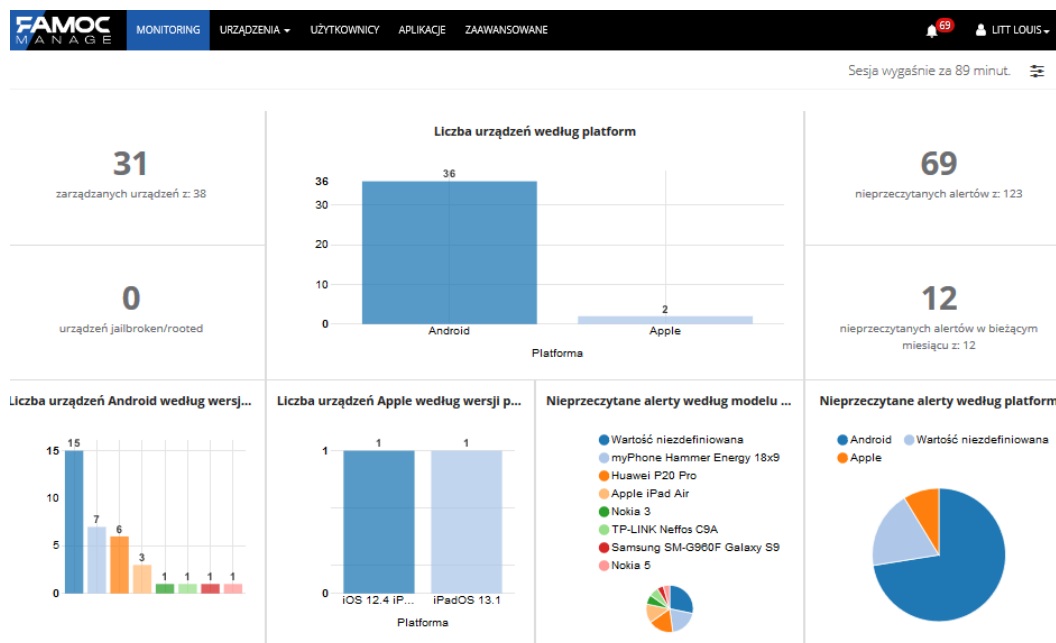
3. Przypisać roli potrzebne uprawnienia poprzez zaznaczenie ich na liście dostępnych funkcjonalności. Po przypisaniu uprawnień pojawią się one w tabeli Przypisane uprawnienia.

4. Zatwierdzić ustawienia przyciskiem Zapisz.

Lista dostępnych uprawnień dostępna jest w dokumencie FAMOC Privileges Guide.

12. Monitoring

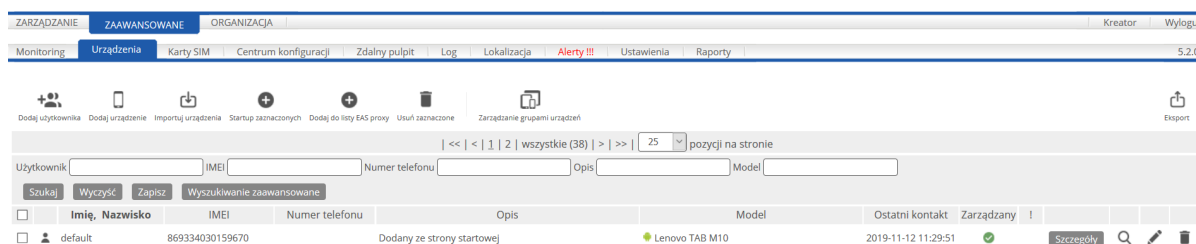
Monitoring wyświetla przegląd raportów FAMOC, pokazuje bieżący status systemu i podaje ogólne statystyki dotyczące FAMOC oraz zarządzanych urządzeń. Dodatkowe informacje o nowym interfejsie znajdują się w dokumentacji: FAMOC UI Guide.



Rysunek 17 Monitoring

13. Urządzenia

Zakładka Urządzenia udostępnia takie dane jak nazwa użytkownika, numer telefonu, opis, model urządzenia czy datę ostatniego kontaktu.



Rysunek 18 Urządzenia

Pasek wyszukiwania urządzeń pomaga zlokalizować telefon komórkowy w systemie. Funkcja Zapisz wyniki umożliwia zachowywanie w pamięci wyników wyszukiwania pod konkretną nazwą. Funkcja Wyszukiwanie zaawansowane – poza zaawansowanym przeszukiwaniem system, pozwala również definiować, które pola mają być widoczne w tabeli głównej. W tym miejscu można również włączyć widok dodanych uprzednio Pół niestandardowych.

Opcja Podłączone do RA znajdująca się pod przyciskiem Szukanie zaawansowane, wyświetla urządzenia podłączone do dostępu zdalnego. Zdalny dostęp umożliwia administratorowi zdalne sterowanie ekranem i klawiaturą urządzenia przenośnego. Po wybraniu opcji "Wyszukiwanie zaawansowane" pola wyboru są wyświetlane obok wszystkich pól wyszukiwania. Zaznaczenie pola wyboru obok elementu powoduje dodanie kolumny do listy urządzeń wraz z odpowiednimi danymi.

Rysunek 19 Wyszukiwanie zaawansowane

W zakładce Urządzenia, dostępne są także następujące przyciski funkcyjne:

- **Dodaj użytkownika** – przenosi do sekcji **ORGANIZACJA** → **Użytkownicy** → **Dodaj użytkownika**
- **Dodaj urządzenie** – umożliwia dodanie nowego urządzenia do systemu FAMOC
- **Importuj urządzenia** – pozwala na grupowy import użytkowników z pliku CSV
- **Startup zaznaczonych** (Rejestracja urządzenia) – umożliwia generowanie kodu startup'u dla wybranych urządzeń, dzięki czemu użytkownicy uzyskają dostęp do strony startowej
- **Dodaj do EAS proxy whitelist** – pozwala na dodanie wybranych identyfikatorów urządzenia (IMEI, UID urządzenia, numer seryjny) do EAS proxy whitelist. Opcja jest dostępna jedynie, jeżeli proxy EAS jest zdefiniowane. Więcej informacji na ten temat znajduje się w rozdziale 21.4.6.
- **Usuń zaznaczone** – umożliwia usunięcie zaznaczonego urządzenia
- **Zarządzaj grupami urządzeń** – przekierowuje do zakładki **Ustawienia** – **Zarządzanie grupami urządzeń**
- **Eksport** – umożliwia eksport danych do pliku CSV (oddzielone przecinkami), .CSV (oddzielone średnikami) lub .TXT.



Rysunek 20 Ikony funkcyjne

13.1 Dodawanie pojedynczego urządzenia

Dodanie nowego urządzenia do systemu wymaga użycia przycisku Dodaj urządzenie w zakładce **ZAAWANSOWANE** → **Urządzenia**, a następnie wprowadzenia następujących danych:

1. Numer telefonu w podzakładce **Karta SIM**³.
2. Użytkownika przypisanego do danego urządzenia w podzakładce **Dane urządzenia**.
3. Modelu (nie jest konieczne dla wszystkich platform obsługiwanych przez agenta bazowego FAMOC).
4. Grupa urządzeń - dodaj nową lub wybierz istniejącą z listy

³ Poprawny format numeru telefonu to: numer kierunkowy kraju + właściwy numer telefonu (np. dla numerów polskich 48600123456)

5. Pozostałe informacje mogą być podane, ale nie jest to wymagane.

Sekcja Dane urządzenia zawiera szczegółowe informacje na temat dodawanego telefonu. Wiele parametrów zostanie zaraportowanych do serwera automatycznie. Inne wymagają ręcznego uzupełnienia, ale nie są wymagane.

Część dotycząca Karty SIM, zawiera szczegóły odnośnie umowy z operatorem. System umożliwia dodanie nowej karty SIM do urządzenia istniejącego już w systemie. Aby to zrobić, należy użyć przycisku Dodaj nową kartę SIM. W przypadku, kiedy do urządzenia chcemy przypisać istniejącą już w systemie kartę SIM, należy wybrać przycisk Włóż istniejącą kartę SIM. Opcja Wyjmij kartę SIM z telefonu, sprawi, że w systemie dana karta SIM nie będzie już przypisana do telefonu.

Aby zarządzać dodanymi urządzeniami należy przeprowadzić proces rejestracji oraz instalacji agentów. Istnieje kilka metod tj. instalacja ręczna (sekcja [13.3](#) oraz [13.4](#)), instalacja ze strony startowej (sekcja [21.4.1](#)) oraz sugerowana metoda instalacji automatycznej opisana w Instrukcji nowego interfejsu.

Nowe urządzenie:

IMEI:		☐ Chcę wpisać numer IMEI samodzielnie.
UID:		☐ Chcę wpisać UID samodzielnie.
Numer seryjny:		
Użytkownik:	Louis Litt	Wybierz użytkownika
Model:		Wybierz producenta telefonu...
Platforma:		Wybierz platformę...

Dane urządzenia Grupy urządzeń **Karta SIM** Własne pola

Numer telefonu (z prefiksem np: 48...):	
Państwo:	Polska
Operator komórkowy:	
IMSI:	
PIN:	
Numer umowy:	
Zakupiona od:	
Data podpisania umowy:	
Data wygaśnięcia umowy:	
Plan taryfowy:	
Roaming:	Nie ☒ Tak ☐
Rozmowy międzynarodowe:	Nie ☒ Tak ☐
Pakiet danych:	Tylko rozmowy ☒ Rozmowy i dane ☐ Tylko dane ☐
Zastrzeżony numer:	Nie ☒ Tak ☐

Rysunek 21 Dodawanie urządzenia

13.2 Dodawanie grupy urządzeń (import)

FAMOC umożliwia dodanie do systemu wielu urządzeń jednocześnie. Opcja ta dostępna jest przy użyciu przycisku Importuj urządzenia w zakładce ZAAWANSOWANE → Urządzenia. System wspiera różne formaty plików importu, a cały proces jest analogiczny do opisywanego wcześniej importu użytkowników i innych zestawów danych (patrz 12.5).

13.3 Zarządzanie pojedynczym urządzeniem

Gdy urządzenie jest dostępne na liście urządzeń można rozpocząć instalację certyfikatów, agenta podstawowego, profilu DM lub innych składników klienta FAMOC na każdym zarządzanym urządzeniu.

Więcej informacji na temat tych funkcji można znaleźć w sekcji 13.4. Szczegóły poszczególnych urządzeń można zobaczyć i zmodyfikować, naciskając przycisk **Zarządzaj** obok urządzenia.

Po naciśnięciu przycisku Zarządzaj wyświetlane są zakładki szczegółów danego urządzenia oraz zarządzania. Ta sekcja umożliwia wykonanie różnych akcji lub wyszukiwanie informacji dla wybranego urządzenia.

Obok tabeli ze szczegółowymi danymi o urządzeniu, w sekcji Szczegóły umieszczone są informacje o przypisanych politykach. Administrator ma także wgląd w ustawienia polityki i jej status. W przypadku, gdy polityka nie jest jeszcze przypisana do danego urządzenia lub jest przestarzała, jest możliwość jej odświeżenia.

Istnieje możliwość również: uruchomienia ponownie urządzenia (dla niestandardowego systemu Android i nadzorowane urządzenia Apple), wyłączenia urządzenia (dla urządzeń Samsung Android i supervised urządzenia Apple) i uruchomienia zdalnego dostępu (jeśli zainstalowany jest odpowiedni agent, szczegóły w rozdziale 17).

The screenshot displays the 'Zarządzanie' (Management) section of the FAMOC 5.17 administrator interface. The top navigation bar includes tabs for 'Monitoring', 'Urządzenia' (selected), 'Karty SIM', 'Centrum konfiguracji', 'Zdalny pulpit', 'Log', 'Lokalizacja', 'Alerty !!!', 'Ustawienia', and 'Raporty'. Below the navigation bar, there are buttons for 'Powrót' (Back) and 'Edycja' (Edit). The main content area is divided into several sections:

- Dane urządzenia** (Device Data): A table listing device information for 'Harvey Specter'.

Użytkownik	Harvey Specter	Informacje
IMEI	866237042178633	
Numer seryjny	9WWDU18C07004263	
Opis	Dodany w trybie Device Owner (NFC, NFC Single)	
Model	Huawei P20 Lite	
Platforma	Android 9.0	
Grupy urządzeń		
Ostatni kontakt	2019-11-06 14:04:20	
Status trybu Device Owner	Aktywny	
Status profilu do pracy	Nie istnieje	
- Przypisana polityka** (Assigned Policy): A table showing the assigned policy.

Nazwa polityki	Zastosowana	Podgląd polityki	Status
Harvey Default	2019-11-06 14:04:17	Q	✓
- Status Exchange proxy**: A section showing the status of the proxy connection.

Status połączenia	✖
-------------------	----------------
- User agent**: A section showing the user agent details.

User agent: Dalvik/2.1.0 (Linux; U; Android 9; ANE-LX1 Build/HUAWEIANE-L21)	
Własność	Urządzenie firmowe
Root	Nie
Status szyfrowania	Zaszyfrowane
Operator komórkowy	
Wersja systemu operacyjnego	9
WLAN MAC	4C:D1:A1:24:7F:22
Status usługi monitorowania aplikacji	Włączona
Data zakupu	
Gwarancja do	
Numer umowy	
Serwisowany przez	
Należy do	
Zakupiony w	
Exchange authorization type	
Exchange server address	
Certificate alias	
KCC Enrollment Token	
PINfixed	

At the bottom of the interface, there are buttons for 'Powrót' (Back) and 'Edycja' (Edit).

Rysunek 22 Zarządzenie pojedynczym urządzeniem

13.3.1 Szczegóły

W tej sekcji znajdują się ogólne informacje na temat zarządzanego urządzenia, takie jak przynależność urządzenia, status jailbreak / root, stan szyfrowania, adres MAC, szczegółową wersję systemu operacyjnego, datę i miejsce zakupu, numer umowy, datę wygaśnięcia gwarancji, partner obsługujący urządzenie oraz właściciel.

13.3.2 Użytkownicy

Zakładka Użytkownicy prezentuje dane o obecnym i poprzednich właścicielach urządzenia.

13.3.3 Aplikacje

Lewe menu sekcji udostępnia następujące funkcjonalności:

- Zainstalowane aplikacje – zakładka prezentuje wszystkie aplikacje zainstalowane z poziomu platformy FAMOC oraz te zaraportowane przez monitor urządzenia wraz ze szczegółami oraz reputacją aplikacji. Każda z aplikacji może zostać Uruchomiona lub Odinstalowana. Kolorem zielonym zaznaczone będą te programy, które zostały zainstalowane przez administratora a ich obecność potwierdzona została w raporcie przesłanym przez Monitor Urządzenia. Czerwony kolor oznacza, że aplikacja, która powinna być obecna na telefonie, nie została rozpoznana przez Monitor Urządzenia (np. została usunięta przez użytkownika). W takim przypadku administrator może użyć funkcji Przeinstaluj wszystko, aby ponownie zainstalować wszystkie aplikacje FAMOC na telefonie i tym samym uzupełnić braki.
- Aplikacje KNOX – w przypadku urządzeń Samsung z aktywnym kontenerem KNOX. Pokazuje aplikacje zainstalowane w KNOX.
- Dostępne w sklepie – zakładka wyświetla podgląd sklepu firmowego wraz z aplikacjami dostępnymi do instalacji. Na liście znajdują się wszystkie aplikacje kompatybilne z urządzeniami i te zawarte w konkretnych sklepach firmowych, przypisane danym grupom użytkowników. Tabela prezentuje także status instalacji i umożliwia następujące działania: instalację, ponowną instalację, uruchomienie, usunięcie.
- Wszystkie zgodne – zakładka prezentuje wszystkie aplikacji dostępne w systemie i zgodne z danym urządzeniem. Tabela uwzględnia status instalacji i umożliwia następujące działania: instalację, ponowną instalację, uruchomienie, usunięcie.
- Odinstalowane aplikacje – zakładka prezentuje listę wszystkich odinstalowanych aplikacji i umożliwia przeglądanie szczegółów oraz reputacji aplikacji.

13.3.4 Polityki

Zakładka wyświetla wszystkie polityki i konfiguracje zastosowane do urządzenia.

Pierwsza tabela prezentuje przypisaną politykę generalną wraz z nazwą, datą przypisania, ostatniej modyfikacji, zastosowania na urządzeniu oraz jej statusem. Administrator ma również możliwość podglądu ustawień danej polityki oraz jej odświeżenia w przypadku, gdy nie została jeszcze zastosowana lub jest nieaktualna. W drugiej tabeli znajdują się wyczerpujące informacje na temat przeprowadzonych konfiguracji wraz z ich statusem.

Szczegóły	Aplikacje	Użytkownicy	Agenty	Polityki	Log	Alerty	Lokalizacja	Bezpieczeństwo	Kopia zapasowa	Karty SIM	Monitor urządzenia	Naprawy
Przypisana polityka												
Nazwa polityki	Utworzona	Ostatnio zmodyfikowana	Zastosowana	Podgląd polityki	Status							
Harvey Default	2018-12-06 14:32:39	2019-08-29 13:10:24	2019-11-06 14:04:17									
Zastosowane konfiguracje												
Nazwa	Typ	Zainstalowane w	Utworzono	Wykonane przez	Ostatni status	Wyłączona						
Tapeta FF 1080p	Ustaw tapetę na ekranie urządzenia	Urządzenie	2019-10-28 12:02:31		2019-10-28 12:05:02							
Powrót	Edycja											

Rysunek 23 Zakładka Polityki

13.3.5 Agenty

Zakładka Agenty zawiera listę aplikacji klienckich FAMOC (agentów) i umożliwia ich instalację, usunięcie lub uruchomienie. Wśród wyświetlanych parametrów znajduje się wersja zainstalowanego oprogramowania, najnowsza dostępna wersja aplikacji, data ostatniego użycia, data pobrania oraz status instalacji.

W zakładce Agenty administrator może wygenerować kod dostępu do trybu serwisowego lub trybu Recovery na urządzeniu, włączenie i wyłączenie logów oraz ich zdalne pobranie.

Szczegóły	Aplikacje	Użytkownicy	Agenty	Polityki	Log	Alerty	Lokalizacja	Bezpieczeństwo	Kopia zapasowa	Karty SIM	Monitor urządzenia	Naprawy
Wygeneruj kod dostępu Włącz tryb serwisowy Włącz logi Pobierz logi z urządzenia Dodawanie urządzeń device owner przez NFC												
Stan logowania: Wyłączone												
Lista agentów												
Agent	Nazwa	Wersja	Najnowsza wersja	Ostatnio uruchomiony	Utworzono	Ściągnięto	Usunięto	Status	Akcje			
Certyfikat												
Agent bazowy	FAMOC Base Agent for Android 6.x and above (Google Play)	5.1.0	5.2.0	2019-11-06 14:04:20	2019-10-28 12:02:26							
Zdalny dostęp	FAMOC Remote Access for Huawei EMUI 5	4.4.0	4.4.0		2019-10-28 12:02:31	2019-10-28 12:04:12						
Agent kopii zapasowej												
Monitor lokalizacji	FAMOC Location for Android	1.8.2	1.8.2		2019-10-28 12:02:31	2019-10-28 12:04:25						
Monitor Użycia	FAMOC Usage Monitor for Android	2.5.0	2.5.0		2019-10-28 12:02:31	2019-10-28 12:04:52						
SecureSource												
Rozszerzenie agenta bazowego												

Rysunek 24 Zakładka Agenty urządzenia

13.3.6 Alerty

W tej zakładce zebrane są wszystkie alerty zgłoszone do systemu przez klienty FAMOC. Tabela przedstawia czas i szczegóły wydarzenia. Dane są wymienione w porządku chronologicznym. Alerty są podzielone na cztery grupy - Przeczytane, Nieprzeczytane, Zignorowane lub Rozwiązane. Po zapoznaniu się ze zgłoszonym problemem, administrator powinien oznaczyć go jako Przeczytany, Zignorowany lub Rozwiązany.

13.3.7 Log

W tej części prezentowana jest lista działań podjętych przez administratora na danym urządzeniu wraz ze statusem i szczegółami.

13.3.8 Lokalizacja

Zakładka daje dostęp do danych dotyczących ostatniego położenia urządzenia. Dostęp do danych lokalizacyjnych wymaga zainstalowania Monitora Lokalizacji. Po jego zainstalowaniu, należy uruchomić aplikację korzystając z zakładki **ZAAWANSOWANY** → **Szczegóły** → **Agenty**. Aktualizować dane można przy użyciu przycisku Pobierz aktualną pozycję w zakładce Lokalizacja.

13.3.9 Bezpieczeństwo

FAMOC zapewnia niezrównany poziom wsparcia bezpieczeństwa na wielu platformach mobilnych, zarządzanych centralnie lub indywidualnie na urządzeniu. Sekcja Bezpieczeństwo danych pokazuje dziennik działań z nazwą akcji, użytą aplikacją/agentem, statusem, datą utworzenia i ostatnim statusem oraz statusem SMS.

Dodatkowo, menu boczne udostępnia następujące funkcjonalności:

- Czyszczenie urządzenia - W tym miejscu administrator może Oznaczyć urządzenie jako skradzione i wyczyścić dane przechowywane na telefonie. Urządzenie, na których czyszczenie danych było wykonane ręcznie można zaznaczyć jako wyczyszczone.

Dla urządzeń iOS dostępna jest także opcja Usunięcia danych korporacyjnych – dzięki niej administrator może automatycznie usunąć wszystkie dane zainstalowane w ramach profilu FAMOC. Dla urządzeń Samsung z kontenerem KNOX dostępny jest dodatkowa opcja Usunięcia danych korporacyjnych kontenera KNOX. W przypadku urządzeń z kontenerem Android for Work dostępny jest dodatkowy przycisk - **Usunięcie danych korporacyjnych - kontener**, który usuwa kontener z urządzenia.

- Blokowanie urządzenia – W tej sekcji administrator ma możliwość zdalnie Zablokować lub Odblokować urządzenie oraz Resetować kod blokady. Opcje dostępne są dla urządzeń Symbian, Android i iOS. Dla urządzeń Samsung z kontenerem KNOX dostępne są dodatkowe przyciski dla Zablokowania kontenera KNOX oraz Resetowania kodu blokady KNOX.

- Zarządzanie certyfikatami - W celu jeszcze lepszego zabezpieczenia infrastruktury mobilnej organizacji, FAMOC oferuje unikalny system wykorzystujący indywidualne certyfikaty dla poszczególnych urządzeń, z możliwością ich zdalnego unieważnienia. Podczas przepływu danych pomiędzy telefonem a serwerem FAMOC, żądanie certyfikatu pochodzi od urządzenia, klucz nie opuszcza urządzenia, dzięki czemu nie ma możliwości podszycia się pod urządzenie poprzez skopiowanie certyfikatu. Ta zakładka prezentuje listę zainstalowanych certyfikatów wraz ze szczegółowymi danymi oraz umożliwia generowanie i zdalną instalację certyfikatu na urządzeniu, jego odnowienie bądź unieważnienie.

13.3.10 Kopia zapasowa

W zakładce Kopia zapasowa znajdują się zapasowe kopie danych pobrane z zarządzanego urządzenia oraz informacje o rodzaju kopii, jej statusie, ścieżce, dacie ostatniego uruchomienia i utworzenia. Można tu również utworzyć oraz przywrócić kopię. Dodatkowo możliwe jest importowanie danych z jednego urządzenia do drugiego.

UWAGA: Utworzenie zapasowej kopii danych wymaga wcześniejszej instalacji aplikacji Backup Agent.

Kopia zapasowa/odzyskiwanie danych

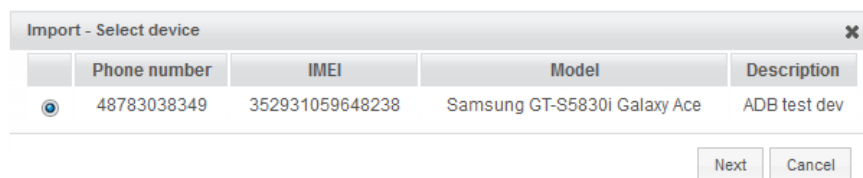
Utworzenie zapasowej kopii danych wymaga stworzenia szablonu backup, czyli określenia, które i jak duże pliki mają być przesłane na serwer. Aby stworzyć nowy szablon backupu, należy użyć przycisku Dodaj nowy, a następnie:

1. Wybrać element, który ma być uwzględniony w backupie (kontakty, kalendarz, folder, SMS-y). W przypadku folderów, należy dodatkowo określić ścieżkę dostępu. Możliwe jest również określenie filtrów np. rodzaju lub maksymalnego rozmiaru plików oraz folderów.
2. Naciśnij Dodaj element
3. Aby wykonać kopię zapasową danych zaznacz odpowiednie elementy i użyj przycisku Backup.
4. Naciśnięcie przycisku Przywróć umożliwia przywracanie plików przechowywanych na serwerze.

Import danych

1. Aby przeprowadzić import danych, należy nacisnąć przycisk Importuj.
2. Wybierz telefon, z którego dane mają być importowane i kliknij Dalej.
3. Dane gotowe do importu pojawią się w tabeli głównej z danymi do backup. Zaznacz plik i ponownie użyj przycisku Importuj.

UWAGA: System umożliwia jedynie import danych pomiędzy urządzeniami należącymi do tego samego użytkownika. Dane z usuniętego urządzenia dostępne są w systemie przez okres jednego miesiąca.



Rysunek 25 Import danych

13.3.11 Karty SIM

Zakładka udostępnia dane o aktualnie aktywnej karcie SIM, historii karty SIM, szczegóły planu taryfowego czy IMSI.

13.3.12 Monitor urządzenia

Monitor urządzenia umożliwia szczegółową analizę parametrów urządzenia (szczegóły urządzenia, hardware, software, procesy, aplikacje, parametry Bluetooth, informacje o dysku i punktach dostępowych itd.)

13.3.13 Naprawy

W tej zakładce znaleźć można szczegółowe informacje na temat przeprowadzanych napraw.

13.3.14 Dane użytkownika

Prezentuje szczegóły połączeń zaraportowanych przez agenta Android Usage Monitor takie jak: typ, data, nr telefonu. Dostępne są również informacje o stanie urządzenia, użyciu aplikacji⁴ oraz historii przeglądarek internetowych. Ta sekcja umożliwia pobieranie wychodzących / przychodzących wiadomości tekstowych i połączeń głosowych.

⁴ Dla urządzeń z Androidem 6.0 oraz wyższym, aplikacje raportowania użycia aplikacji wymagane jest włączenie "Usługi monitorowania aplikacji" na urządzeniu.

13.3.15 Zarejestrowane połączenia

Zakładka przedstawia szczegóły połączenia zarejestrowane przez aplikację Symbian Audit Agent, takie jak typ połączenia, data lub numer telefonu. Ta sekcja umożliwia pobieranie wychodzących/przychodzących wiadomości tekstowych i połączeń głosowych.

UWAGA: Pliki rejestrowane są w formacie AMR⁵ (Adaptive Multi-Rate audio codec), dlatego odtworzenie nagrań wymaga odpowiedniego oprogramowania.

13.4 Instalowanie certyfikatów i agenta podstawowego na poszczególnych urządzeniach

Instalacja Instalowanie certyfikatu, agenta podstawowego FAMOC, zdalnego dostępu FAMOC, FAMOC Backup Agent lub FAMOC Security Agent na jednym urządzeniu możliwa jest poprzez kliknięcie przycisku Zainstaluj w podzakładce Agenty w sekcji ZAAWANSOWANE.

Szczegóły

Aplikacje

Użytkownicy

Agenty

Polityki

Log

Alerty

Lokalizacja

Bezpieczeństwo

Kopia zapasowa

Karty SIM

Monitor urządzenia

Naprawy

Wygeneruj kod dostępu

Włącz tryb serwisowy

Włącz logi

Pobierz logi z urządzenia

Dodawanie urządzeń device owner przez NFC

Stan logowania: Wyłączone

Lista agentów

Agent	Nazwa	Wersja	Najnowsza wersja	Ostatnio uruchomiony	Utworzono	Ściągnięto	Usunięto	Status	Akcje
Certyfikat									
Agent bazowy	FAMOC Base Agent for Android 6.x and above (Google Play)	5.1.0	5.2.0	2019-11-06 14:04:20	2019-10-28 12:02:26				
Zdalny dostęp	FAMOC Remote Access for Huawei EMUI 5	4.4.0	4.4.0		2019-10-28 12:02:31	2019-10-28 12:04:12			
Agent kopii zapasowej									
Monitor lokalizacji	FAMOC Location for Android	1.8.2	1.8.2		2019-10-28 12:02:31	2019-10-28 12:04:25			
Monitor Użycia	FAMOC Usage Monitor for Android	2.5.0	2.5.0		2019-10-28 12:02:31	2019-10-28 12:04:52			
SecureSource									
Rozszerzenie agenta bazowego									

Powrót

Edycja

Rysunek 26 Instalacja agentów na pojedynczym urządzeniu

Rekomendowana kolejność instalacji jest następująca:

1. Certyfikat (dla niezaufanych certyfikatów)
2. Agent Bazowy (łącznie z agentem bezpieczeństwa na platformy Android i iOS)
3. Zdalny Dostęp
4. Backup Agent
5. Monitor Lokalizacji
6. Usage monitor
7. Rejestrator połączeń

Status instalacji poszczególnych aplikacji określają następujące symbole:

- Agent został zainstalowany poprawnie
- Nowsza wersja oprogramowania jest dostępna w systemie
- Agent nie jest zainstalowany na urządzeniu
- Użytkownik odmówił instalacji
- Aplikacja została wysłana na telefon
- Trwa instalacja

⁵ Kodek audio Adaptive Multi-Rate to opatentowany schemat kompresji danych audio zoptymalizowany pod kątem kodowania mowy.

- Rozpocznij sesję zdalnego dostępu
- Wyślij konfigurację na telefon w przypadku, gdy zawiodła konfiguracja automatyczna

Więcej informacji na temat procesu instalacji można znaleźć w 16.1.

14. Karty SIM

Zakładka Karty SIM daje dostęp do wszystkich kart SIM włączonych do usługi FAMOC, zarówno wykorzystywanych i niewykorzystywanych aktualnie przez urządzenia zdalne. W tej sekcji możliwe jest edytowanie szczegółów karty oraz usunięcie jej z systemu

W tabeli głównej dostępne są następujące ikony:

- Dodaj nową kartę SIM, umożliwia rejestrację nowych kart w systemie.
- Importuj kartę SIM umożliwia importowanie danych zbiorczych poprzez przesyłanie sformatowanych plików.
- Wstaw umożliwia przypisanie karty SIM do wybranego urządzenia mobilnego.

Użytkownik	Numer telefonu	IMSI	Model	Opis urządzenia
Harvey BYOD	48795503174	260021621926791		
Harvey Specter	48694866457	260021764289900		
Harvey Specter	48661820011	260021462694197	Samsung SM-G955F Galaxy S8 Plus	

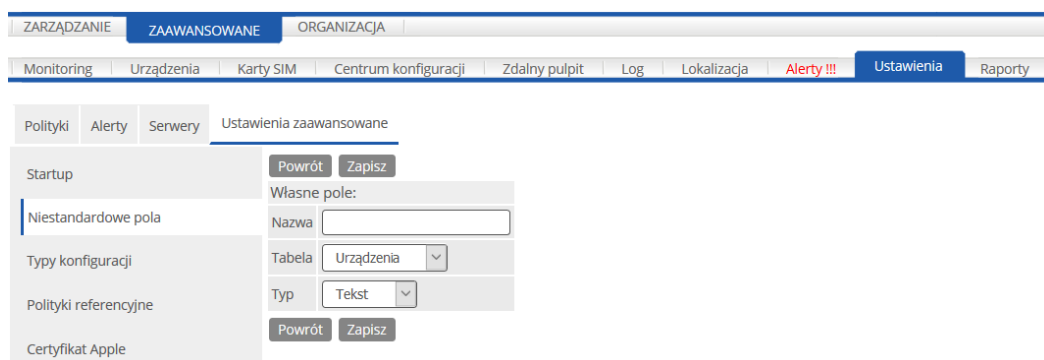
Rysunek 27 Zakładka Karty SIM

W momencie gdy administrator chce dodać niestandardowe pola do widoku kart SIM, powinien przejść do sekcji Zaawansowane / Ustawienia / Ustawienia zaawansowane i dodać w zakładce Niestandardowe pol żądany element do tabeli kart SIM.

Nazwa	Typ	Tabela
Certificate alias	Tekst	Urządzenia
Exchange authorization type	Słownik	Urządzenia
Exchange server address	Tekst	Urządzenia
KCC Enrollment Token	Tekst	Urządzenia
PINfixed	Tekst	Urządzenia
user.mail	Tekst	Użytkownicy

Rysunek 28 Niestandardowe pola

Następnie administrator może przejść ponownie do zakładki Zaawansowane / Urządzenia i kliknąć export, pola niestandardowe są zawarte w oknie dialogowym eksportu danych.



Rysunek 29 Edycja pól niestandardowych

15. Centrum konfiguracji

Centrum konfiguracji FAMOC umożliwia wykonywanie masowych operacji na zarządzanych telefonach. Obejmuje to instalowanie aplikacji, wykonywanie kopii zapasowych oraz konfigurowanie urządzeń.

Sekcja Centrum konfiguracji składa się z ośmiu modułów: Agenty, Aplikacje, Sklep firmowy store, Konfiguracje, Wiadomości, Kopie zapasowe, Pakiety oraz Zestawy pakietów.

15.1 Agenty

Zakładka Agenty umożliwia jednocześnie instalowanie certyfikatów, Agenta podstawowego, Zdalnego dostępu, Agenta kopii zapasowych, programu Security Agent, Monitora lokalizacji, Monitora użycia, Rejestratora połączeń i Add-onu na dowolnej liczbie urządzeń. Szczegóły dotyczące każdej pozycji, w tym numer wersji i liczbę udanych instalacji, wyświetlone są tutaj. W przypadku telefonów z różnymi systemami operacyjnymi, takimi jak Symbian, Windows Mobile lub UIQ, odpowiednia wersja aplikacji musi zostać wybrana przed instalacją. Ta sekcja wyświetla również listę operacji związanych z każdym agentem i umożliwia skonfigurowanie apletu.

15.1.1 Instalacja certyfikatu

Certyfikat służy do zapewnienia bezpieczeństwa transmisji danych, jest niezbędny do prawidłowego działania agentów. Tak jak w przypadku każdej innej aplikacji, Certyfikat można instalować na pojedynczym telefonie bądź na grupie telefonów jednocześnie.

UWAGA: W przypadku, gdy serwer korzysta z certyfikatu preinstalowanego na telefonach komórkowych (np. VeriSign), ten krok można pominąć.

1. Naciśnij Instaluj, aby wysłać certyfikat do urządzeń mobilnych.
2. Wybierz urządzenia mobilne, na których chcesz zainstalować certyfikat, naciskając przycisk Dodaj telefony.
3. Wybierz urządzenia z okna pop-up pokazującego wszystkie obsługiwane urządzenia. Wybierając przycisk Grupy, można dokonać wyboru grupowego. Aby ułatwić wybór urządzenia, można zastosować filtry.
4. Przed wysłaniem można sprawdzić listę wybranych urządzeń. FAMOC pozwala również wybrać, czy instalacja powinna zostać wykonana natychmiast czy później.

Rysunek 30 Instalacja certyfikatu

15.2 Aplikacje

Zakładka Aplikacje umożliwia tworzenie repozytorium aplikacji dla każdej organizacji. Dodatkowe funkcje obejmują instalowanie, usuwanie, uruchamianie i raportowanie aplikacji (przeglądanie listy operacji związanych z każdą aplikacją oraz listę urządzeń z zainstalowaną aplikacją). Ponadto ta sekcja wyświetla licencje aplikacji.

15.2.1 Dodawanie aplikacji z Apple App Store

1. W zakładce Aplikacje użyj przycisku **Dodaj aplikację**.
2. Zaznacz opcję **Dodaj aplikację z Apple App Store**.
3. Wprowadź nazwę aplikacji i naciśnij Dalej.
4. Lista aplikacji z Apple App Store, odpowiadających podanej wcześniej nazwie, zostanie wyświetlona.
5. Zaznacz odpowiednią aplikację i naciśnij Dalej.
6. Szczegóły aplikacji zostaną wyświetlone wraz z możliwością ustawienia:
 - a. Grupa aplikacji, do której ma zostać przypisana aplikacja
 - b. Udostępnij w sklepie firmowym
7. Kliknij Zapisz, aby dodać aplikację do repozytorium, lub kliknij przycisk Zapisz i edytuj, aby dodać aplikację i utworzyć formularz edycji.

UWAGA: Istnieje możliwość stworzenia niestandardowej konfiguracji dla każdej aplikacji: zakładka Konfiguracja w formularzu edycji aplikacji.

15.2.2 Dodawanie aplikacji z Google Play

1. W zakładce Aplikacje użyj przycisku **Dodaj aplikację**.
2. Zaznacz opcję **Dodaj aplikację z Google Play**.
3. Wprowadź nazwę aplikacji i naciśnij Dalej.
4. Zostanie wyświetlona lista aplikacji z Google Play, odpowiadających podanej wcześniej nazwie.
5. Zaznacz odpowiednią aplikację i naciśnij Dalej.
6. Szczegóły aplikacji zostaną wyświetlone wraz z możliwością ustawienia:
 - a. Grupa aplikacji, do której ma zostać przypisana aplikacja
 - b. Udostępnij w sklepie firmowym
7. Kliknij Zapisz, aby dodać aplikację do repozytorium, lub kliknij przycisk Zapisz i edytuj, aby dodać aplikację i otworzyć formularz edycji. Zarządzanie grupami aplikacji

15.2.3 Dodawanie aplikacji niestandardowych

1. W zakładce Aplikacje użyj przycisku Dodaj aplikację.
2. Wybierz opcję Dodaj aplikację niestandardową.
3. Wpisz Nazwę, Opis oraz Wersję.
4. Wybierz Grupę aplikacji z dostępnych pozycji lub utwórz nową używając ikony "+".
5. Przy opcji Dostępność w sklepie firmowym zaznacz pole Dostępna dla wszystkich, jeśli aplikacja ma być widoczna dla wszystkich urządzeń lub przypisz grupy użytkowników lub grupy urządzeń, dla których aplikacja powinna być dostępna.
6. Wgraj plik z lokalnego komputera używając przycisku Wybierz plik. Przy instalacji aplikacji na telefonach javowych, potrzebne jest także załączenie pliku instalacyjnego .jad. W celu umożliwienia użytkownikom końcowym pobranie aplikacji z AppStore'a lub Google Play, zaznacz opcję Instalacja ze sklepu i podaj właściwy link⁶.
7. FAMOC udostępnia domyślną ikonę aplikacji pojawiającej się w AppStore. Przycisk Zmień pozwala na wgranie innej grafiki.
8. Każda aplikacja wymaga wybrania odpowiedniego system operacyjny oraz modeli telefonów. Zaznacz na liście wszystkie Platformy i Modele, z którymi dana aplikacja jest kompatybilna. Niektóre platformy zostaną wybrane automatycznie przez system jako sugestie - mogą zostać zmienione.
9. W zakładce Zdjęcia aplikacji możliwe jest wgranie przykładowych zrzutów ekranu pokazujących wygląd i funkcjonalność aplikacji.
10. W Opcjach zaawansowanych uzupełnij Zasady i warunki korzystania z aplikacji.
11. Jeśli używasz telefonów z systemem Windows Mobile, zdefiniuj Start command, dzięki której Agent Bazowy FAMOC będzie mógł uruchamiać aplikację (Symbian: UID3 pliku, Windows Mobile: nazwa aplikacji (wyświetlana na urządzeniu)).
12. Możliwe jest także wpisanie treści wiadomości, które pojawią się na telefonie użytkownika przed i po instalacji.

⁶ Funkcjonalność dostępna obecnie tylko na urządzeniach z systemami Android oraz iOS.

13. W zakładce **Konfiguracje** administrator może wybrać niestandardowe parametry konfiguracyjne lub predefiniowaną konfigurację (możliwość wyboru jednej konfiguracji z listy). W przypadku niektórych aplikacji (dostępność zależy od aplikacji) można używać konfiguracji zarządzanych przez system Android. Po udanej instalacji aplikacji, odpowiednia konfiguracja jest wysyłana do urządzenia (w oparciu o kompatybilność platformy). Konfiguracja jest wysyłana za każdym razem, gdy aplikacja jest instalowana ponownie.

14. W podzakładce **Licencje**, administrator ma możliwość dodania licencji do aplikacji. Dodatkowo, z tego miejsca możliwe jest zastosowanie kodów programu Apple Volume Purchase Program (VPP). Licencje mogą być wgrane z pliku lub wklejone bezpośrednio przy użyciu przycisku Wklej.

Format wgrywanego pliku lub wklejanej licencji:

- Pierwsza linijka powinna zawierać nagłówek klucza licencji (oddzielony średnikami jeśli jest kilka części klucza licencji)

- Kolejne linie – klucz licencji

Kody programu Apple VPP powinny zawierać jedną kolumnę (pierwszy wiersz to nagłówek klucza licencji, kolejne to kody)⁷.

Przykładowy plik

Code
CCXFJ8989PQA
ZSPAJ7979NFF

15. Kliknij przycisk **Zapisz**, aby dodać aplikację do repozytorium aplikacji.

15.2.4 Zarządzanie grupami aplikacji

Przycisk Zarządzanie grupami aplikacji kieruje do zakładki ZAAWANSOWANE → Ustawienia → Ustawienia zaawansowane → Zarządzanie grupami aplikacji, w której administrator ma możliwość utworzenia i zarządzania grupami aplikacji (patrz 21.4.7).

15.2.5 Instalacja aplikacji na telefonie

Instalacja aplikacji trzeciej jest analogiczna do opisanej wcześniej instalacji aplikacji FAMOC (patrz 14)

1. Wybierz aplikację, która ma być zainstalowana i rozpocznij proces, wybierając przycisk Instaluj znajdujący się obok niej.
2. Używając przycisku **Dodaj urządzenia**, stwórz listę urządzeń, na których ma być zainstalowana aplikacja. Jeśli Agent Bazowy jest już zainstalowany na telefonach, rekomendowane jest użycie go jako metody instalacji. Określ, czy aplikacja ma być zapisana w pamięci telefonu czy na karcie pamięci i zdecyduj, czy dana operacja ma być wykonana natychmiast czy po upływie określonego czasu. Po ustaleniu wszystkich parametrów **Wyślij aplikację**.
3. W zależności od konfiguracji agenta bazowego (**Potwierdzenie, Informacja, Cichy**), użytkownicy mogą być poproszeni o zatwierdzenie akcji na swoich urządzeniach
4. Status operacji dostępny jest w Logu zdarzeń.

⁷ Dodatkowe informacje na temat programu VPP, znaleźć można na stronie: <http://www.apple.com/business/vpp>

15.3 Konfiguracje

Zakładka **Konfiguracje** umożliwia przygotowywanie i przeprowadzanie zdalnej konfiguracji na dowolnej liczbie urządzeń. W tabeli głównej zakładki znajdują się wstępnie przygotowane konfiguracje, pogrupowane względem platformy mobilnej oraz typu konfiguracji, gotowe do wysłania na urządzenia. Drzewo zależności w lewym menu zapewnia łatwy dostęp do dostępnych konfiguracji.

Kliknięcie w ikonę Pokaż stan polityki wyświetla na ekranie szczegóły dotyczące danej konfiguracji (typ, opis, itd.) oraz stan zaimplementowanej polityki (liczba urządzeń zgodnych z polityką, liczba urządzeń niezgodnych z aktualną polityką, liczba urządzeń, na których nie powiodła się implementacja polityki) wraz z opcją ponownego przesłania polityki na urządzenia w przypadku jej przedawnienia lub niepoprawnej instalacji.

Status polityki

Dane konfiguracji

Nazwa konfiguracji:	iOS safari kiosk
Rodzaj konfiguracji:	Konfiguracja podstawowego profilu iOS
Opis konfiguracji:	
Data ostatniej modyfikacji:	2019-10-10 16:04:44

Stan polityki

Urządzenia zgodne z polityką:	1		
Urządzenia niezgodne z aktualną polityką:	0		
Urządzenia, na których nie powiodła się implementacja polityki:	1		<button>Wyślij ponownie</button>

Wyślij ponownie do wszystkich Zamknij

Rysunek 31 Konfiguracje

Konfiguracje dostępne w FAMOC są podzielone na następujące grupy:

Rodzaje konfiguracji	
Polityka z serwera BES	Import polityk z serwerów BlackBerry Enterprise Server
Sieć/Połączenia	Konfiguracje połączeń sieciowych m.in. synchronizacja z serwerem SyncML Http, konfiguracja punktów dostępowych, ustawienia VoIP SIP oraz Bluetooth, konfiguracje WLAN.

Bezpieczeństwo	Obejmuje ustawienia parametrów ochrony antywirusowej i podejmowanie działań mających na celu zapewnienie bezpieczeństwa urządzenia, takich jak szyfrowanie urządzenia, wymazywania danych, blokada urządzenia i wiele innych.
Poczta elektroniczna	Konfiguracja m.in. TouchDown, MailForExchange oraz IBM Lotus Notes Traveler umożliwiające zdalną synchronizację poczty, zadań, kalendarza i kontaktów za pośrednictwem sieci 3G / HSDPA lub WiFi.
Narzędzia	Konfiguracje narzędzi urządzeń zdalnych takich jak aparat, zegar, alarm, przeglądarka internetowa, klucze rejestru.
iOS	Kompleksowa konfiguracja dedykowana na urządzenia iOS
KNOX	Konfiguracje kontenera KNOX
Personalizacja urządzenia	Konfiguracje umożliwiające brandowanie i dostosowywanie urządzeń przez dodanie logotypu, zmianę tapety lub ustawień przeglądarki internetowej, zarządzanie wyglądem strony domowej
Exchange policies	Konfiguracja kont pocztowych Microsoft Exchange ActiveSync ⁸

Tabela 2 Typy konfiguracji

15.3.1 Dodanie nowej konfiguracji

Aby dodać nową pozycję do listy, użyj przycisku **Dodaj konfigurację**.

Kliknij **Wybierz typ konfiguracji**, aby wybrać szablon konfiguracji.

Dodaj unikalną nazwę (od teraz będzie widoczna w systemie pod tą nazwą) i uzupełnij wymagane parametry.

The screenshot shows the 'Centrum konfiguracji' (Configuration Center) interface. At the top, there are tabs for Monitoring, Urządzenia, Karty SIM, Centrum konfiguracji (active), Zdalny pulpit, Log, Lokalizacja, Alerty !!!, Ustawienia, and Raporty. Below these are sub-tabs: Agenty, Aplikacje, Sklep firmowy, Konfiguracje (active), Wiadomości, Backup, Pakiety, and Pakiety pakietów. The main content area is titled 'Wybierz typ konfiguracji' and includes a search bar and a 'Platformy' dropdown. A list of configuration templates is displayed, each with a description, a platform/OS version, and a 'Base Agent' status, followed by a 'wybierz' button. The templates include configurations for Exchange, TouchDown, mySecureMail, and various mobile OSes like Android, iOS, and Windows Mobile. The left sidebar shows a tree view of configuration categories, with 'Poczta elektroniczna' (Email) expanded.

Rysunek 32 Dodawanie nowej konfiguracji

W zakładce **Sklep firmowy** możesz wybrać, czy konfiguracja ma być dostępna dla wszystkich, czy tylko dla przypisanych grup użytkowników lub grup urządzeń. Możesz także wybrać opcję Instaluj lub Aktualizuj

⁸ Więcej informacji na temat konfiguracji kont pocztowych Microsoft Exchange ActiveSync znaleźć można w dokumencie: FAMOC Administrator Guide Appendix: FAMOC Exchange Web Service Addon Installation Guide

konfigurację automatycznie (zostanie ona automatycznie zainstalowana lub zaktualizowana po wprowadzeniu jakichkolwiek zmian).

Rysunek 33 Ustawienia sklepu firmowego

15.3.2 Wysłanie konfiguracji na urządzenia zdalne

Gotowe konfiguracje można wysyłać na telefony komórkowe za pomocą przycisku Wyślij. Wybierz urządzenia mobilne, które chcesz użyć, klikając przycisk Dodaj telefony. Wybierz opcję Metoda instalacji: Część osobista lub Kontener. Operacja jest podobna do każdej poprzednio opisanej instalacji⁹.

15.4 Wiadomości

Zakładka Wiadomości umożliwia administratorom FAMOC wysyłanie wiadomości na dowolną liczbę urządzeń. FAMOC zapewnia SMS-y bootstrap informujące użytkowników urządzeń mobilnych o implementacji systemu.

1. Aby stworzyć nowy komunikat, użyj przycisku **Dodaj wiadomość**.
2. Wprowadź **Nazwę**.
3. Wybierz typ wiadomości: **SMS** lub **Wiadomość push**. (Dla wiadomości push wybierz rodzaj wiadomości: informacyjny lub z potwierdzeniem)
4. Wprowadź treść wiadomości.
5. Aby wysłać wiadomość, naciśnij przycisk **Wyślij**.

15.5 Backup

Zakładka Kopia zapasowa przechowuje kopie danych z urządzeń mobilnych na centralnym serwerze FAMOC. Umożliwia to przywrócenie danych po utracie danych lub wymianie urządzenia.

⁹ Więcej informacji znajduje się w 16.1

ZARZĄDZANIE ZAAWANSOWANE ORGANIZACJA

Monitoring | Urządzenia | Karty SIM | Centrum konfiguracji | Zdalny pulpit | Log | Lokalizacja | Alerty

Agenty | Aplikacje | Sklep firmowy | Konfiguracje | Wiadomości | Backup | Pakiety | Pakiety pakietów

Powrót Zapisz

Nowy wzorzec backupu:

Nazwa:

Typ	Ścieżka	Maksymalna wielkość	Maksymalna wielkość pliku	Backupowane pliki	Pliki wyłączone z backupu
Contacts		20 MB			X
Calendar		20 MB			X
Sms		50 MB			X

Dodaj nowy element:

Typ danych: Katalog na dysku

ścieżka do katalogu np. /home/data C:/PHOTO/

Dodaj element

Powrót Zapisz

Rysunek 33 Wzorzec backupu

1. Aby stworzyć schemat tworzenia zapasowej kopii danych, użyj przycisku **Dodaj wzorzec backupu**.
2. Określ nazwę konfiguracji.
3. Stwórz listę elementów, które mają być pobrane z telefonu i przesłane na serwer (kontakty, kalendarz, SMS, katalog z dysku). System umożliwia dodatkowo określenie parametrów backupowego pliku. Możliwe jest ustalenie maksymalnej wielkości backupu i pojedynczego pliku oraz ustalenie, które pliki mają być wyłączone z backupu.
4. Naciśnij **Dodaj element**.
5. Zapisz wzorzec, który zostanie automatycznie dodany do listy gotowych schematów.
6. Aby wykonać kopię zapasową, naciśnij przycisk **Wykonaj w repozytorium**.

System wspiera obecnie następujące platformy:

- Android
- Apple iPhone
- RIM BlackBerry
- Symbian S60
- Microsoft Windows Mobile
- JAVA
- Samsung Bada
- Symbian UIQ

16. Zdalny pulpit

Zdalny dostęp to bardzo bezpieczne i łatwe w użyciu rozwiązanie, które pozwala administratorowi zdalnie rozwiązywać problemy z urządzeniami przenośnymi za pośrednictwem połączenia transmisji danych (np. Internetu), umożliwiając administratorowi przeglądanie ekranu i przejmowanie kontroli nad klawiaturą.

Zdalny dostęp wymaga zainstalowania agenta podstawowego w telefonie. Aby uzyskać informacje na temat instalacji agenta podstawowego, patrz 16.1.

16.1 Instalacja zdalnego dostępu

Tak jak inne aplikacje klienckie FAMOC, zdalny dostęp może być zainstalowany:

- W sekcji **ZAAWANSOWANE** → **Urządzenia** → **Szczegóły** → **Agenty**
- W zakładce **ZAAWANSOWANE** → **Centrum konfiguracji** → **Agenty**

Patrz: sekcje 14 i 16.1

Proces jest analogiczny do opisywanych wcześniej instalacji agentów, konfiguracji i aplikacji.

16.2 Uruchomienie sesji zdalnego dostępu

Aby rozpocząć sesję dostępu zdalnego, przejdź do karty **Dostęp zdalny**. Telefony z zainstalowanym agentem zdalnego dostępu będą miały włączony przycisk **Uruchom**.

ZARZĄDZANIE

ZAAWANSOWANE

ORGANIZACJA

Monitoring

Urządzenia

Karty SIM

Centrum konfiguracji

Zdalny pulpit

Log

Lokalizacja

Alerty !!!

Ustawienia

Raporty

Sesje

Pozostałe dostępne urządzenia

Lp	Model telefonu	Platforma	Użytkownik	Opis	IMEI	Liczba sesji	
1	Zebra TC51 TC56	Android 6.0	Harvey Secure	Added from startup page	353857080043694		Uruchom
2	myPhone Hammer Energy 18x9	Android 7.0	Harvey Specter		354788082627730		Uruchom
3	Huawei Mate 20 Lite	Android 8.1	Donna Paulsen		869814035283773		Uruchom
4	Motorola Moto G	Android 7.1	Harvey Specter		355661081875437		Uruchom
5	Samsung SM-J530G Galaxy J5 2017	Android 7.0 - Samsung	Donna Paulsen	Dodany ze strony startowej	356437085292062		Uruchom

Rysunek 34 Zakładka zdalny pulpit

Połączenie może być zainicjowane poprzez:

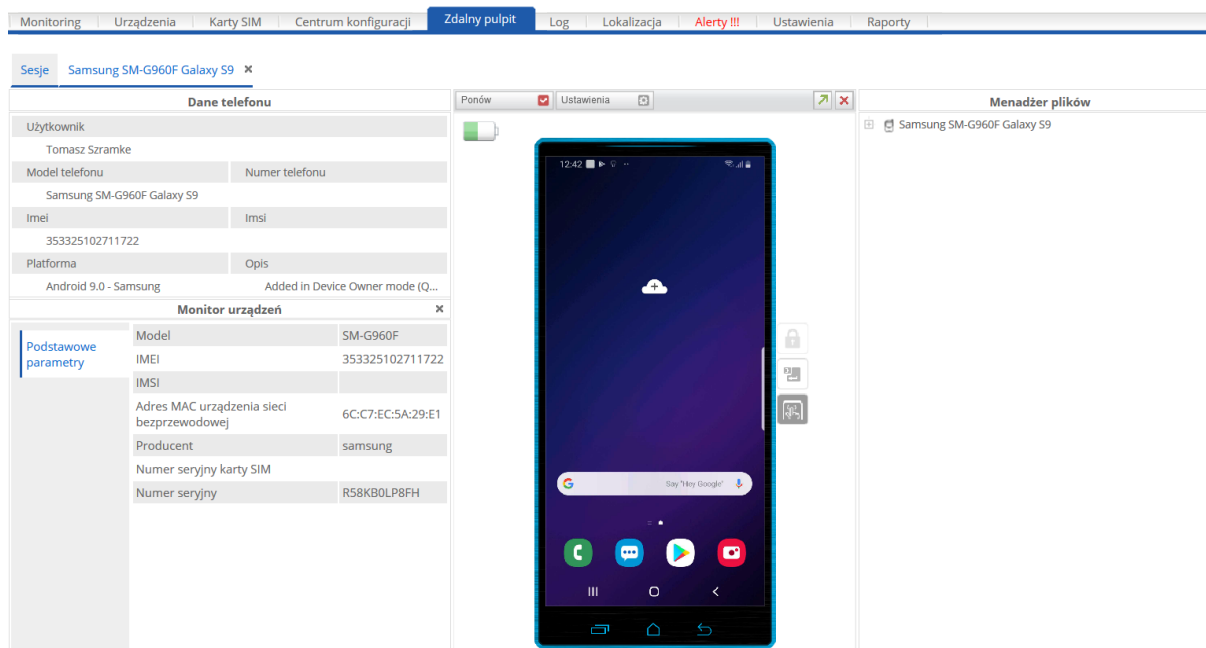
- Kliknięcie łącza **Uruchom** obok telefonu
- Właściciela urządzenia przez uruchomienie aplikacji **Zdalny dostęp** na telefonie

Po nawiązaniu połączenia między telefonem a serwerem FAMOC dostępny będzie link Rozpoczęcia sesji zdalnego dostępu.

Możliwe jest również uruchomienie zdalnego dostępu w sekcji **Zarządzaj** na karcie **Urządzenia**.

16.3 Panel zdalnego pulpitu

Kliknięcie łącza **Rozpocznij sesję** aktywuje panel zdalnego dostępu. Gdy administrator jest podłączony do urządzenia użytkownika końcowego, zdalne narzędzia bezprzewodowej diagnostyki i zarządzania dają administratorowi jeszcze więcej możliwości niż fizyczna obecność. Użytkownik telefonu może zobaczyć wszystkie podejmowane czynności na ekranie i może zakończyć połączenie w dowolnym momencie, rozłączając lub zamykając agenta dostępu zdalnego w telefonie.



Rysunek 35 Panel zdalnego dostępu

Przycisk **Zdalna blokada telefonu** umożliwia zdalne blokowanie i odblokowanie klawiatury telefonu. Funkcja ta jest szczególnie przydatna, gdy w czasie przerwy w sesji zdalnego dostępu, telefon przełącza się z trybu czuwania i blokuje klawiaturę automatycznie.

Przycisk **Włącz/Wyłącz klawiaturę komputera** umożliwia przełączenie się z klawiatury telefonu na klawiaturę PC administratora. Przycisk przydatna m.in. podczas wprowadzania parametrów konfiguracyjnych.

Symbol ekranu dotykowego umożliwia zarządzanie telefonem z ekranem dotykowym za pośrednictwem panelu zdalnego dostępu FAMOC.

Panel wyświetla również boczne przyciski telefonu komórkowego, a także stan naładowania baterii urządzenia i siłę sygnału.

16.3.1 Monitor urządzenia

Monitor urządzenia¹⁰ daje wgląd w techniczne dane o urządzeniu. Pozwala tym samym na szybką identyfikację zaistniałych problemów np. z wydajnością i niekompatybilnością. Zakres identyfikowanych parametrów jest uzależniona od system operacyjnego podłączonego telefonu.

16.3.2 Menadżer plików

Menadżer plików¹¹ umożliwia zarządzanie plikami i folderami na urządzeniu zdalnym. Oprócz operacji na plikach, takich jak kopiowanie, usuwanie, zmiana nazwy, Menedżer plików umożliwia przesyłanie i pobieranie plików. Ta funkcja może być używana np. do zastąpienia plików konfiguracyjnych lub analizy logów aplikacji.

¹⁰ Monitor urządzenia jest obecnie wspierany przez platformy Apple iOS, Android, Windows 10 Mobile, Windows 8.1+, RIM BlackBerry, Symbian S60, Windows Mobile and Symbian UIQ

¹¹ Menedżer plików jest obecnie wspierany przez platformy Android, Symbian S60, Windows Mobile oraz Symbian UIQ

16.3.3 Konfiguracje

Panel zdalnego dostępu umożliwia administratorowi włączanie / wyłączanie podświetlania przycisków telefonu i ustawienie jakości zrzutów ekranu w celu dostosowania wymagań przepustowości do wolniejszych połączeń.

17. Log

FAMOC rejestruje wszelkie działania wykonywane na telefonach w dzienniku systemowym. Dostęp do dziennika organizacji można uzyskać na karcie Dziennik i zawiera następujące informacje:

- Rodzaj podejmowanej akcji
- Aplikacja/Agent, którego dotyczyła operacja
- Datę utworzenia
- Ostatni status podjętego działania: data i godzina ostatniego statusu
- Status: operacja zakończona pomyślnie / żądanie wysłane / operacja nie powiodła się
- Wiadomość: wysłanie / wysłanie nie powiodło się
- Opis telefonu
- Numer IMEI
- Numer telefonu
- Użytkownik urządzenia
- ID operacji
- Działania: możliwe działania na konkretnej operacji (ponawianie, anulowanie)

Dodatkowo, dane przedstawione w logu mogą być sortowane według następujących kategorii: operacje niezakończone, wykonane poprawnie, nieudane, oczekujące, oczekujące na operacje zależną, anulowane, rozpoczęte, wysłane żądanie, rozpoczęte pobieranie, aplikacje uruchomione oraz oczekujące na użytkownika.

Można przejść bezpośrednio do szczegółów urządzenia, klikając kolumnę IMEI.

Dzienniki aktywności dla poszczególnych urządzeń są dostępne na karcie Urządzenia, klikając przycisk Zarządzaj obok wybranego telefonu.

Log operacji

Status operacji: Pokaż wszystkie 25 pozycji na stronie

Akcja	Komponent	Utworzono	Utworzył	Ostatni status	Status	Wiadomość	ID	ID grupy	Akcje
Uruchomiony	Zdalny dostęp	2019-11-12 12:40:34		2019-11-12 12:40:34	Wykonano poprawnie		197764		
Uruchom	Zdalny dostęp	2019-11-12 12:40:27		2019-11-12 12:40:33	Wykonano poprawnie	Wysłano	197762		
Uruchomiony	Zdalny dostęp	2019-11-08 14:40:36		2019-11-08 14:40:36	Wykonano poprawnie		197746		
Uruchom	Zdalny dostęp	2019-11-08 14:40:32		2019-11-08 14:40:36	Wykonano poprawnie	Wysłano	197745		
Uruchomiony	Zdalny dostęp	2019-11-08 14:37:34		2019-11-08 14:37:34	Wykonano poprawnie		197744		

Rysunek 36 Log zdarzeń

18. Lokalizacja

Zakładka Lokalizacja umożliwia identyfikowanie pozycji urządzenia oraz wyznaczanie trasy przebytej w określonym odcinku czasu. Historię danych lokalizacji można eksportować jako plik CSV lub TXT.

Rysunek 37 Lokalizacja

19. Alerty

Zakładka Alerty daje wgląd w przeczytane i nieprzeczytane komunikaty alarmowe zgłoszone do systemu dotyczące m.in. wykrycia nieprawidłowej konfiguracji na telefonie, rozpoznania aplikacji znajdującej się na czarnej liście czy zgłoszenia przez użytkownika problemu z telefonem.

Tabela podaje czas i szczegóły zdarzenia, jak również parametry urządzenia, którego dotyczy zgłoszenie. Dane są wymienione w porządku chronologicznym. Po przeczytaniu alertu, administrator może skorzystać z opcji naprawy sugerowanej przez system. Przycisk napraw to, wyświetla opis problemu i rekomenduje odpowiednie działania.

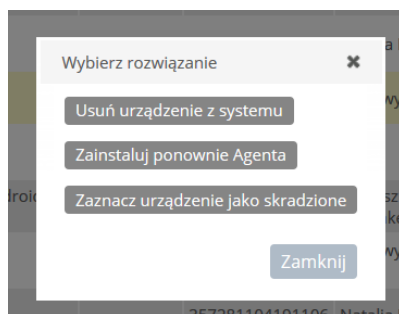
Górne menu pozwala grupować alerty odpowiednio do następujących kategorii: nieprzeczytane, przeczytane, zignorowane i rozwiązane. Gdy administrator zapozna się z alertem, powinien zostać oznaczony jako przeczytany, nieprzeczytany, zignorowany lub rozwiązany za pomocą odpowiedniego przycisku.

FAMOC umożliwia filtrowanie alertów na podstawie dostępnych kategorii: Szczegóły, Komunikat, Numer telefonu, IMEI, Użytkownik, Opis, Model, Platforma, Typ alertu.

Kliknięcie alertu powoduje przekierowanie do danych danego telefonu.

Alerty są również widoczne w zakładce ZAAWANSOWANE → Urządzenia. Każdy problem raportowany do systemu zaznaczony jest kolorem czerwonym i ikoną .

ZARZĄDZANIE									
ZAAWANSOWANE ORGANIZACJA									
Monitoring Urządzenia Karty SIM Centrum konfiguracji Zdalny pulpit Log Lokalizacja Alerty III Ustawienia Raporty									
Kreator Wyloguj 5.2.0									
Nieprzeczytane Przeczytane Zignorowane Rozwiązane									
Oznacz jako przeczytane Oznacz jako zignorowane Oznacz jako rozwiązane									
<< < 1 2 3 wszystkie (74) > >> 25 pozycji na stronie Szukaj: Filtruj według typu alertu: --Wybierz-- Szukaj Wyczyść									
Alert		Urządzenie							
		Szczegóły	Komunikat	Numer telefonu	IMEI	Użytkownik	Opis	Model	Platforma
☐	Stworzony								
☐	2019-11-10 13:25:25	2019-11-12 08:40:29	KNOX zaraportował zmianę statusu licencji.	Błąd wewnętrzny.	354607087262469	Paweł Kamiński	Added in Device Owner mode (QR Code)	Samsung SM-A520F Galaxy A5 2017	Android 8.0 - Samsung
☐	2019-11-08 14:10:37		Aplikacja została odinstalowana przez użytkownika	com.android.chrome	352766094586963	Paweł Kamiński	Added in Device Owner mode (QR Code)	Sony Xperia XA2	Android 9.0
☐	2019-11-08 14:10:37		Aplikacja została odinstalowana przez użytkownika	com.fancyon.strongswan	352766094586963	Paweł Kamiński	Added in Device Owner mode (QR Code)	Sony Xperia XA2	Android 9.0
☐	2019-11-08 14:07:10		Aplikacja została odinstalowana przez użytkownika	com.android.chrome	354607087262469	Paweł Kamiński	Added in Device Owner mode (QR Code)	Samsung SM-A520F Galaxy A5 2017	Android 8.0 - Samsung
☐	2019-11-08 14:05:03	2019-11-12 02:33:04	Dostępna aktualizacja oprogramowania urządzenia	A520FOXUBCS1/A520FOXABCS1/A520FOXUBCS1	354607087262469	Paweł Kamiński	Added in Device Owner mode (QR Code)	Samsung SM-A520F Galaxy A5 2017	Android 8.0 - Samsung
☐	2019-11-08 14:05:03	2019-11-12 02:33:04	Dostępna aktualizacja oprogramowania urządzenia	A520FOXUBCS1/A520FOXABCS1/A520FOXUBCS1	354607087262469	Paweł Kamiński	Added in Device Owner mode (QR Code)	Samsung SM-A520F Galaxy A5 2017	Android 8.0 - Samsung
☐	2019-11-08 14:04:58	2019-11-08 14:10:31	Znaleziono identyfikator zablokowanej aplikacji!	Photo editor (Trojan Android - Photo Editor)	352766094586963	Paweł Kamiński	Added in Device Owner mode (QR Code)	Sony Xperia XA2	Android 9.0
☐	2019-11-08 13:59:53	2019-11-11 09:12:10	Znaleziono identyfikator zablokowanej aplikacji!	Photo Editor (Trojan Android - Photo Editor)	354607087262469	Paweł Kamiński	Added in Device Owner mode (QR Code)	Samsung SM-A520F Galaxy A5 2017	Android 8.0 - Samsung



Rysunek 38 Alerty

UWAGA: FAMOC pozwala administratorowi określić, jakie komunikaty powinny być zgłaszane do systemu oraz do kogo powinny być przekierowane. Zarządzanie Alertami umożliwia zakładka ZAAWANSOWANE → Ustawienia → Alerty.

20. Ustawienia

W Ustawieniach administrator może zarządzać konfiguracją aplikacji klienckich FAMOC (agentów), synchronizować system z serwerami zewnętrznymi oraz definiować parametry alertów zgłaszanych do serwera. Obejmuje następujące sekcje: Polityki, Alerty, Serwer, Zaawansowane.

20.1 Polityki

W tej sekcji administrator może zdefiniować parametry polityk FAMOC i skonfigurować parametry Agenta Bazowego. System umożliwia tworzenie kilku odrębnych szablonów polityk dla różnych grup użytkowników. Poza ustawieniami Agenta Bazowego, do polityki można dodać określone agenty, konfiguracje i aplikacje¹². Domyślna polityka podstawowa zostanie zastosowana do wszystkich urządzeń, które nie przynależą do grup przypisanych do innych polityk podstawowych.

Domyślna polityka					
Nazwa szablonu polityki	Utworzony w	Ostatnio zmieniany			
Empty - silent mode	2014-03-03 12:40:00	2019-11-08 11:52:25			

Nazwa szablonu polityki	Priorytet	Przypisane grupy użytkowników	Przypisane grupy urządzeń	Utworzony w	Ostatnio zmieniany	
preconf_COBO	↓		COBO	2019-10-21 08:05:55	2019-10-21 08:52:24	🔍 🚩 ✎ 🗑
preconf_COPE	↑ ↓		COPE	2019-10-21 07:58:16	2019-11-08 13:51:11	🔍 🚩 ✎ 🗑
krzysiek_wp	↑ ↓	km		2019-10-18 12:28:57	2019-10-29 13:39:42	🔍 🚩 ✎ 🗑

Rysunek 39 Główny widok polityk

Każda polityka jest podzielona na kilka sekcji:

- **Ustawienia podstawowe** - ogólne ustawienia, takie jak nazwa, priorytet, włączone usługi lub harmonogramy
- **Przypisane grupy** - grupy urządzeń i / lub użytkowników przypisanych do polityki
- **Elementy polityki** - aplikacje i konfiguracje przypisane do polityki
- **Opcje bezpieczeństwa** - ustawienia zabezpieczeń, w tym np. możliwość zablokowania Bluetooth, ustawień telefonu, ustawień czasu, menedżera plików, przeglądarki internetowej, instalatora aplikacji.
- **Profil do pracy** - możliwość włączenia i skonfigurowania kontenera na urządzeniu
- **Zaawansowane** - zaawansowane ustawienia polityki, pola szczegółów urządzenia w Agencie bazowym, zasady tworzenia kopii zapasowych i użytkowania

¹² Więcej informacji na temat tworzenia nowych szablonów polityk, można znaleźć w dokumencie FAMOC Administrator Guide Appendix: Policy Templates.

Rysunek 40 Ustawienia podstawowe polityki

20.2 Alerty

Zakładka **Alerty** umożliwia administratorowi zarządzanie ustawieniami alertów FAMOC.

20.2.1 Typy alertów

Sekcja **Typy alertów** pozwala definiować, które z wykrytych nieprawidłowości raportowane są do systemu i tym samym, o których zdarzeniach alarmowany jest administrator. Wybrane rodzaje komunikatów widoczne będą w razie ich rozpoznania w sekcji Alerty (**ZAAWANSOWANE** → **Alerty**), Logu systemowym (**ZAAWANSOWANE** → **Log**), logu zdarzeń na konkretnym urządzeniu (**ZAAWANSOWANE** → **Urządzenia** → **Szczegóły** → **Log**) oraz w zakładce **Urządzenia**.

20.2.2 Przekierowanie alertów

W tej sekcji administrator ma możliwość ustawienia reguł przekazywania powiadomień (np. Alerty mogą być przekazywane do właściciela urządzenia). Administrator może określić, które powiadomienia powinny być automatycznie kierowane do określonych użytkowników. FAMOC umożliwia także ustawianie natychmiastowego powiadamiania SMS-em i e-mailem, a także przekazywanie alertów do zewnętrznego SNMP lub systemu syslog.

W przypadku przekazywania komunikatów użytkownikom (lub grupie użytkowników), każdy z nich musi mieć przypisany numer telefonu/adres e-mail. Przesyłanie alertów na serwer SNMP wymaga skonfigurowania serwera w zakładce **ZAAWANSOWANE** → **Ustawienia** → **Serwery**.

Alert może zostać przekazany na zewnętrzny serwer Syslog. Aby przesłać alerty do zewnętrznego syslog, należy zdefiniować odpowiedni serwer na zakładce **ZAAWANSOWANE** → **Ustawienia** → **Serwery**.

System pozwala dowolnie definiować parametry wiadomości, np. od kogo przyszła wiadomość, na jaki adres wysłać odpowiedź, tytuł i treść wiadomości. Wprowadzone dane użyte będą podczas wysyłania powiadomienia drogą mailową lub SMS-ową, w momencie, gdy zdefiniowany alert pojawi się w systemie.

Dodatkowo jest możliwość użycia kilku tokenów (token będzie podmieniony danymi pobranymi z serwera FAMOC). Dostępne tokeny:

- Tytuł: `_ALERT_ID_` - nowy alert

- Treść wiadomości email:

_ALERT_ID_ - ID alertu

_ALERT_CREATED_ON_ - data utworzenia alertu

_ALERT_DESCRIPTION_ - opis alertu

_ALERT_MESSAGE_ - komunikat

_PHONE_NUMBER_ - numer telefonu

IMEI - IMEI telefonu

MODEL - model telefonu

USER - imię i nazwisko użytkownika

COMPANY - firma użytkownika

USERGROUPS - lista grup użytkownika

_DEVICE_DESCRIPTION_ - opis urządzenia

_GEN_POLICY_ - nazwa polityki generalnej urządzenia

_SEC_POLICY_ - nazwa polityki bezpieczeństwa urządzenia

- Treść wiadomości SMS: _ALERT_ID_ - ID alertu

_ALERT_DESCRIPTION_ - opis alertu

_ALERT_MESSAGE_ - komunikat

USER - imię i nazwisko użytkownik

Nowe przekierowanie

Nazwa:

Ustawienia wiadomości | Typy alertów | Użytkownicy | Grupy | Serwery SNMP | Serwery Syslog

Ustawienia wiadomości

Od (nazwa):

Od (email):

Odpowiedz do (email):

Tytuł:

Treść wiadomości email:

Wiadomość z systemu FAMOC.

Wygenerowano nowy alert:

ID alertu: _ALERT_ID_
 Data: _ALERT_CREATED_ON_
 Opis alertu: _ALERT_DESCRIPTION_
 Komunikat: _ALERT_MESSAGE_
 Numer telefonu: _PHONE_NUMBER_
 IMEI: _IMEI_

Treść wiadomości SMS: (111)

[FAMOC ALERT][ID: _ALERT_ID_] [_ALERT_DESCRIPTION_]

Treść wiadomości syslog:

Rysunek 41 Ustawienia przekierowania alertów

20.2.3 Lista zabronionych aplikacji

Sekcja umożliwia zarządzanie czarną listą aplikacji (blacklist), chroniącą użytkowników przed złośliwym oprogramowaniem, spywarem czy wirusami. Funkcja opiera się na działaniu Monitora Urządzenia i raportuje do systemu czy aplikacja znajdująca się na czarnej liście, została wykryta na telefonie. W celu uzyskiwania

aktualnych raportów, zaleca się zaplanowanie sesji monitorowania urządzeń np. raz dziennie lub raz w tygodniu w zakładce **ZAAWANSOWANE** → **Ustawienia** → **Agenci** → **Agent Bazowy**.

Aby włączyć monitorowanie obecności konkretnej aplikacji na telefonach użytkowników:

1. Użyj przycisku Dodaj nową aplikację do czarnej listy.
2. Określ nazwę aplikacji.
3. Wybierz odpowiednią platformę mobilną.
4. W zależności od platformy mobilnej, określ wyrażenia poszukiwane podczas sesji Monitora urządzenia.:
 - a. BlackBerry: Application Full Name
 - b. Symbian S60: Application UID, Application Full Name, Application Short Name, Application File
 - c. Apple iOS: Process Name
 - d. Android: Application Full Name, Application File
 - e. Windows Mobile: Application Full Name
5. Zapisz ustawienia.

21.2.4 Lista dozwolonych aplikacji

Sekcja umożliwia zarządzanie listą dozwolonych aplikacji (whitelist) w oparciu o dane z monitora urządzenia. Pozwala na weryfikację, czy na urządzeniu zainstalowano aplikacje spoza listy i wysłanie alertu do administratora w przypadku wykrycia niedozwolonej aplikacji

Aby dodać element do listy dozwolonych aplikacji:

1. Naciśnij przycisk Dodaj listę dozwolonych aplikacji.
2. Wybierz nazwę dla listy dozwolonych aplikacji.
3. Wybierz platformę, dla której ma być utworzona lista.
4. Ustaw listę jako Aktywną.
5. Wybierz aplikacje:
 - a. Ręcznie – poprzez kliknięcie przycisku Dodaj (pojawi się okno z polem tekstowym).
 - b. Z danych monitora urządzenia – poprzez kliknięcie przycisku Wybierz z monitora urządzenia. W tym przypadku pojawi się nowe okno z listą istniejących sesji monitora dla urządzenia. W tym oknie można przeglądać listę aplikacji i dodać je do listy po kliknięciu przycisku Wybierz. W ten sposób wszystkie aplikacje wybrane z sesji monitora urządzenia zostaną dodane do listy dozwolonych aplikacji.

Alerty są wysyłane w przypadku każdej aktywnej listy dozwolonych aplikacji dla danej platformy.

21.3 Serwery

Sekcja umożliwia dodanie do systemu i synchronizację lub usuwanie takich serwerów zewnętrznych jak Exchange, SNMP, Certificate Authority.

Użyj przycisku Dodaj serwer aby ustawić konfigurację serwera Exchange, SNMP, Certificate Authority lub Syslog i wprowadź wymagane parametry.

Po zapisaniu ustawień serwer pojawia się w repozytorium i możliwe jest zsynchronizowanie.

Na liście serwerów, przy pozycji Certificate Authority, istnieje możliwość wygenerowania i zainstalowania certyfikatu CA na wielu urządzeniach jednocześnie. Dodatkowo administrator może przeglądać urządzenia,

na których został zainstalowany certyfikat. Lista certyfikatów jest porządkowana przez kolumnę z datą ich wygaśnięcia. Popup udostępnia także opcję odnowienia certyfikatów.

Parametr	Opis
Nazwa	Nazwa serwera
Adres	Adres IP serwera Exchange
Port	Port serwera Exchange
Interwał	Interwał synchronizacji FAMOC-Exchange
Ilość zapamiętanych synchronizacji z serwerem Exchange	Ilość zsynchronizowanych danych dostępnych na serwerze
Użytkownik Web Service	Nazwa użytkownika Web Service
Hasło użytkownika Web Service	Hasło użytkownika Web Service
Typ synchronizacji	Wszystkie dane (użytkownicy i urządzenia)/urządzenia istniejących użytkowników
Synchronizuj tylko istniejące urządzenia FAMOC	Tak/Nie
Synchronizuj urządzenia, które odzywały się do serwera Exchange w ciągu...	Dzień/Trzy dni/Tydzień/Dwa tygodnie/Miesiąc/Rok

Tabela 3 Parametry konfiguracyjne serwera Exchange

Parametr	Opis
Nazwa	Nazwa serwera
Adres	Adres IP serwera SNMP
Port	Port serwera SNMP
Interwał	Interwał synchronizacji FAMOC-SNMP

Tabela 4 Parametry konfiguracji serwera SNMP

Parametr	Opis
Typ	Typ serwera (Microsoft CA)
Nazwa	Nazwa serwera
Adres	Adres IP serwera CA
Port	Port serwera CA
Interwał synchronizacji	Interwał synchronizacji FAMOC- serwer Certificate Authority

Odwołaj certyfikaty urządzenia po operacji czyszczenia	Tak/Nie, jeśli zaznaczone certyfikaty zostaną odwołane po czyszczeniu urządzenia
Długość klucza certyfikatu	Rozmiar klucza (1024, 2048 ...). Urządzenia iOS oraz Symbian akceptują jedynie długość klucza 1024 lub 2048. W przypadku ustawienia większej wartości, na tych urządzeniach będzie generowany klucz o maksymalnej dopuszczalnej długości.
Nazwa komputera serwera	Nazwa komputera serwera
Nazwa Certificate Authority	Nazwa Certificate Authority
Użytkownik Web Service	Użytkownik Web Service
Hasło użytkownika Web Service	Hasło użytkownika Web Service
Domena Certificate Authority	Domena Certificate Authority
Szablon certyfikatu	Szablon certyfikatu
Nazwa własna (CN)	Nazwa własna certyfikatu. Można uzupełnić pole lub wybrać z bazy FAMOC. Możliwy jest wybór trzech części: • Pole z bazy FAMOC (np. Login lub pole niestandardowe) • Separator (kropka, dwukropek albo @) • Dodatkowe pole z bazy FAMOC
Kraj(C)	Kraj
Miejscowość (L)	Miejscowość
Województwo (ST)	Województwo
Organizacja (O)	Nazwa organizacji
Jednostka organizacyjna (OU)	Jednostka organizacyjna
Dodatkowy atrybut SAN (DNS)	Subject Alternative Name. Można uzupełnić pole lub wybrać z bazy FAMOC. Możliwy jest wybór trzech części: • Pole z bazy FAMOC (np. Login lub pole niestandardowe) • Separator (kropka, dwukropek albo @) • Dodatkowe pole z bazy FAMOC
Dodatkowy atrybut UPN	User Principal Name. Można uzupełnić pole lub wybrać z bazy FAMOC. Możliwy jest wybór trzech części: • Pole z bazy FAMOC (np. Login lub pole niestandardowe) • Separator (kropka, dwukropek albo @) • Dodatkowe pole z bazy FAMOC
Źródło certyfikatu	Z pliku / Stworzony i podpisany przez CA
Plik certyfikatu (.PFX)	Wgraj plik certyfikatu
Hasło pliku PFX	Ustaw hasło pliku PFX

Tabela 5 Parametry konfiguracyjne serwera CA (Microsoft CA)

Parametr	Opis
Typ	Typ serwera (FAMOC CA)
Nazwa	Nazwa serwera
Adres	Adres IP serwera CA
Port	Port serwera CA
Interwał synchronizacji	Interwał synchronizacji FAMOC-Serwer CA
Odwołaj certyfikaty urządzenia po operacji czyszczenia	Tak/Nie, jeśli zaznaczone certyfikaty zostaną odwołane po czyszczeniu urządzenia
Długość klucza certyfikatu	Rozmiar klucza (1024, 2048 ...). Urządzenia iOS oraz Symbian akceptują jedynie długość klucza 1024 lub 2048. W przypadku ustawienia większej wartości, na tych urządzeniach będzie generowany klucz o maksymalnej dopuszczalnej długości.
Plik certyfikatu PKCS#12 (.PFX, .P12)	Plik certyfikatu
Hasło PKCS#12	Hasło do pliku certyfikatu
Okres	Ważność wystawianych certyfikatów
Nazwa własna (CN)	Nazwa własna certyfikatu. Można uzupełnić pole lub wybrać z bazy FAMOC. Możliwy jest wybór trzech części: • Pole z bazy FAMOC (np. Login lub pole niestandardowe) • Separator (kropka, dwukropek albo @) • Dodatkowe pole z bazy FAMOC
Kraj (C)	Kraj
Miejscowość(L)	Miejscowość
Województwo (ST)	Województwo
Organizacja(O)	Nazwa organizacji
Jednostka organizacyjna (OU)	Jednostka organizacyjna
Dodatkowy atrybut SAN (DNS)	Subject Alternative Name. Można uzupełnić pole lub wybrać z bazy FAMOC. Możliwy jest wybór trzech części: • Pole z bazy FAMOC (np. Login lub pole niestandardowe) • Separator (kropka, dwukropek albo @) • Dodatkowe pole z bazy FAMOC
Atrybut UPN	User Principal Name. Można uzupełnić pole lub wybrać z bazy FAMOC. Możliwy jest wybór trzech części: • Pole z bazy FAMOC (np. Login lub pole niestandardowe) • Separator (kropka, dwukropek albo @) • Dodatkowe pole z bazy FAMOC
Wykorzystanie klucza	Użytkownik może zaznaczyć sekcje, które będą wymagały do oblokowania certyfikatu

Rozszerzone wykorzystanie klucza	Użytkownik może oznaczyć bardziej zaawansowane sekcje, które będą wymagały certyfikatu do odblokowania
OID (Dodaj rozszerzenie)	Użytkownik może zdefiniować sekcję niestandardową za pomocą kodu OID, który będzie wymagał certyfikatu do odblokowania
Źródło certyfikatu	Z pliku / Stworzony i podpisany przez CA
Plik certyfikatu (.PFX)	Wgraj plik certyfikatu.
Hasło pliku PFX	Ustaw hasło pliku PFX

Tabela 6 Parametry konfiguracyjne serwera CA (FAMOC CA)

Parametr	Opis
Nazwa	Nazwa serwera
Adres	Adres IP danego serwera Syslog
Port	Port serwera Syslog
Interwał	Interwał synchronizacji z serwerem Syslog

Tabela 7 Parametry konfiguracyjne Syslog

21.4 Ustawienia zaawansowane

Sekcja umożliwia zarządzanie ogólnymi parametrami serwera FAMOC, takimi jak konfiguracja strony instalacyjnej, dodanie do panelu pól niestandardowych, zarządzanie typami konfiguracji oraz definiowanie polityk referencyjnych.

21.4.1 Startup

Funkcja Startup umożliwia instalację systemu FAMOC na urządzeniach zdalnych poprzez wykorzystanie interfejsu sieciowego. W sytuacjach, gdy standardowa opcja instalacyjna (link WAP-push) nie ma zastosowania, możliwe jest pobranie mobilnych aplikacji klienckich z internetowej strony startowej, przy wykorzystaniu wbudowanej przeglądarki. Po wprowadzeniu adresu strony startowej należy zalogować się przy pomocy danych użytkownika lub hasła globalnego. Następnie użytkownik może ręcznie pobrać certyfikat, Agenta Bazowego i pliki konfiguracyjne. Podczas instalacji Agenta konieczne będzie wyrażenie zgody na instalację z nieznanych źródeł.

Parametr	Opis
Ustawienia ogólne	
Strona startowa	Określ czy instalacja na urządzeniach mobilnych przez interfejs web będzie dozwolona Wartość domyślna: Włączona
Adres strony startowej	Prostsza nazwa domeny, która stanowić będzie alternatywny link do strony startowej. Wartość domyślna: adres serwera/nazwa organizacji Rekomendowany adres strony
Ustawienia zaawansowane	

Dodatkowy pełny adres	Alternatywny, pełny URL, który nie podlega edycji Ta opcja jest przestarzałą
Nazwa serwera w serwerze Apache dla wirtualnego hosta	Prostsza nazwa domeny, będąca jednocześnie alternatywnym linkiem do strony startowej
Tytuł strony startowej	Edytowalny tytuł strony startowej, nazwa domyślna: FAMOC
Preferowane źródło instalacji agentów	Wybierz źródło, skąd ma być pobrany plik agenta. Dostępne opcje: FAMOC lub Sklep Google Play.
Nagłówek strony startowej	Edytowalny nagłówek strony startowej, domyślnie: FAMOC
Wymagane podanie opisu urządzenia	Wymagaj opisu urządzenia na stronie startowej. Opcja domyślnie odznaczona
Pokaż certyfikat na stronie startowej	Określa czy link do pobrania certyfikatu jest wyświetlony na stronie startowej Sets if certificate download link is shown on startup page. Dostępne opcje: • Na podstawie certyfikatu serwera – ogólne ustawienia będą użyte (jeśli serwer korzysta z zaufanego certyfikatu – nazwa nie będzie ukazywana) • Nie pokazuj certyfikatu • Pokaż certyfikat
Czas wygaśnięcia kodu startowego	Domyślnie nieustawiony. Możliwe wartości to: 1 dzień, 1 tydzień, 2 tygodnie, 1 miesiąc
Ustawienia logowania	
Wymagane zalogowanie się użytkownika	Wybór opcji wymusi na użytkowniku wpisanie loginu i hasła w celu uzyskania dostępu do strony startowej (dane LDAP/AD będą użyte jeśli umożliwiono synchronizację). Oznaczenie opcji wyświetla dwa dodatkowe parametry: Globalne hasło lub kod startowy i Tylko kod startowy. Wartością domyślną jest wybór opcji wymagania logowania
Globalne hasło lub kod startowy	Globalne hasło do strony startowej – wspólne dla wszystkich użytkowników. Jeśli administrator użyje tego parametru, użytkownik będzie musiał podać hasło odwiedzając stronę. Możliwe jest także użycie kodu startowego. Jeśli opcja jest zaznaczona i pole hasła puste, wówczas dostęp do strony nie będzie zabezpieczony hasłem.
Tylko kod startowy	Dostęp do strony startowej tylko z kodem startowym dla urządzenia, generowanym z zakładki ZAAWANSOWANE → Urządzenia
Ustawienia użytkownika	
Użytkownik domyślny	Wybierz domyślnego użytkownika, do którego przypisane będzie urządzenie. Jeśli użytkownik nie będzie wybrany, użytkownik będzie proszony o wybór odpowiedniej opcji w momencie otwarcia strony startowej.
Ustawienia grupy urządzeń	
Domyślna grupa urządzeń	Umożliwia wybór domyślnej grupy, do której urządzenia są przypisywane. Jeżeli żadna z grup nie jest zaznaczona użytkownik zostanie zapytany o wybór opcji z listy w momencie otwarcia strony startowej.

Ustawienia pakietu instalacyjnego	
Tylko Base Agent z politykami	Na stronie dostępny będzie wyłącznie Agent Bazowy wraz z konfiguracją. Ta opcja jest wartością domyślną
Wybierz pakiet do instalacji	Umożliwia wybór pojedynczego pakietu, który będzie automatycznie instalowany na urządzeniach odwiedzających stronę. (zobacz 16.6)
Automatyczny wybór pakietu w zależności od platformy	Udostępnia kilka pakietów określonych dla różnych platform mobilnych. FAMOC automatycznie identyfikuje platformę urządzenia odwiedzającego stronę i dostosowuje pakiet.
Pozwól użytkownikowi wybrać pakiet	Umożliwia ręczny wybór pakietu instalacyjnego przez użytkownika odwiedzającego stronę.
Ustawienia strony powitalnej	
Pokazuj stronę powitalną	Wybór opcji wyświetla dwa dodatkowe parametry. Wartość domyślna: brak strony powitalnej
Wiadomość powitalna	Tekst wyświetlany przy uruchamianiu strony startowej. W tym polu można wprowadzić kod HTML: ([LINK]...[/LINK] lub [EMAIL]... [/EMAIL]. Brak tekstu skutkuje nie wyświetlaniem wiadomości powitalnej. Użytkownik zostanie przekierowany na standardową stronę startową zawierającą łącza do pobierania składników klienta FAMOC.
Link z wiadomością powitalną	Zamiast wiadomości powitalnej wyświetla się adres wprowadzony w tym polu
Wiadomość powitalna z adresem e-mail	Zamiast wiadomości powitalnej wyświetla się adres e-mail wprowadzony w tym polu.
Przycisk powitalny	Tekst wyświetlany na przycisku umożliwiającym użytkownikowi uruchomienie instalacji np. Dalej, Kontynuuj, Akceptuj.
Strona powitalna z potwierdzeniem	Umożliwia utworzenie pola zatwierdzenia, które użytkownik musi wybrać, aby zarejestrować urządzenie.
Prośba o potwierdzenie	Personalizowana wiadomość z polem do odhaczenia. Domyślnie: Zaakceptuj warunki użytkowania.
Ustawienia wiadomości startupowej	
Od (nazwa)	Nazwa nadawcy. Domyślnie Serwer FAMOC
Od (email)	Adres nadawcy
Odpowiedz do (email)	Adres odpowiedzi
Tytuł	Tytuł wiadomości
Treść wiadomości email	Wiadomości email z możliwością wykorzystania tokenów
Treść wiadomości SMS	Treść wiadomości SMS z linkiem startupowym

Tabela 8 Startup

W przypadku określenia ustawień pakietu na "Użyj wybranego pakietu", "Automatyczny wybór pakietu" lub "Pozwól użytkownikowi wybrać pakiet" konieczne jest najpierw utworzenie Pakietu Bootstrap i Zestawu

pakietów (patrz 16.7). Podczas tworzenia pakietu ważne jest, aby zaznaczyć opcję Zezwól na Bootstrap. Wówczas taki zestaw operacji, dostępny będzie w sekcji Startup.

21.4.2 Niestandardowe pola

Ta sekcja umożliwia dodawanie do panelu administratora pól niestandardowych, dzięki którym system udostępni opis dodatkowych parametrów w tabeli urządzeń, kart SIM lub grup użytkowników. Formatem danych wpisywanych do nowego pola może być tekst, liczba, data lub specjalnie utworzony słownik (patrz 11.6).

1. Użyj przycisku Dodaj pole.
2. Podaj Nazwę pola.
3. Wybierz tabelę systemową, w której ma się wyświetlać nowe pole (Urządzenia/ Karty SIM/ Grupy).
4. Określ obowiązujący w polu format danych (tekst/ liczba/ hasło/ data/ słownik).
5. Zapisz ustawienia.

21.4.3 Typy konfiguracji

Główne repozytorium wyświetla drzewo istniejących grup typów konfiguracji (predefiniowane i niestandardowe) z niestandardowymi typami konfiguracji. Administrator może wykonać pewne operacje na każdym elemencie drzewa (z wyłączeniem wstępnie zdefiniowanych elementów). Listę można rozwinąć lub zwinąć za pomocą znaczników "-" / "+" (po lewej stronie nazwy grupy); domyślnie jest rozwinięty.

Zakładka pozwala administratorowi dodawać nowe typy konfiguracji i grupy typów konfiguracji do FAMOC. Możliwe jest również tworzenie typów konfiguracji przy użyciu niestandardowych plików lub plików z narzędzia iPhone Configuration Utility. Utworzone szablony pojawią się w sekcji ZAAWANSOWANE → Centrum konfiguracji → Konfiguracje → Dodaj konfigurację¹³.

21.4.4 Polityki referencyjne

W tej części możliwe jest dodanie do systemu nowej polityki referencyjnej lub opisać własną politykę IT, a następnie porównać zakres spełniania określonych wytycznych w zakładce ZARZĄDZANIE → Raporty → IT Policies benchmark. Aby zdefiniować nowy zestaw standardowych procedur zarządzania urządzeniem:

1. Użyj przycisku Dodaj politykę.
2. Wprowadź Nazwę.
3. Określ zalecane wartości przy każdym z elementów polityki takie jak czas bezczynności, wymagana długość hasła, reguły szyfrowania pamięci, harmonogram tworzenia kopii zapasowych itp.
4. Zapisz ustawienia.

21.4.5 Certyfikat Apple

Zdalne zarządzanie urządzeniami Apple wymaga wykonania uprzednio następujących działań¹⁴:

- Rejestracja na stronie Apple i zdobycie identyfikatora Apple ID¹⁵

¹³Więcej informacji na temat tworzenia nowych typów konfiguracji w systemie FAMOC, można znaleźć w dokumencie Custom Configuration Types.

¹⁴ Instrukcje dotyczące generowania certyfikatów Apple dostępne są w dokumencie FAMOC iOS Configuration Guide.

¹⁵ Identyfikator Apple można uzyskać na stronie: <https://appleid.apple.com/>

- Wygenerowanie żądania certyfikatu CSR (Certificate Signing Request) z poziomu platformy FAMOC.
- Podpisanie pliku CSR na portalu partnerskim FancyFon (Krok można pominąć, jeżeli licencja z certyfikatem została wgrana na serwer).
- Wgranie podpisanego CSR na stronie Apple i wygenerowanie certyfikatu Apple.
- Wgranie certyfikatu Apple na serwer FAMOC przez konsolę administratora.

Zakładka Certyfikat Apple umożliwia generowanie CSR oraz wgrywanie certyfikatu Apple na serwer FAMOC.

Aby wygenerować CSR, użyj przycisku Wygeneruj żądanie certyfikatu. Po wygenerowaniu CSR w tym samym miejscu możliwe będzie wgranie gotowego certyfikatu Apple na serwer FAMOC

Przycisk Usuń, umożliwia skasowanie certyfikatu. Jednak opcja ta dostępna jest wyłącznie w sytuacji, gdy żadne urządzenie nie korzysta z danego certyfikatu, ponieważ skutkowałoby to brakiem możliwości nawiązania z nim ponownie kontaktu.

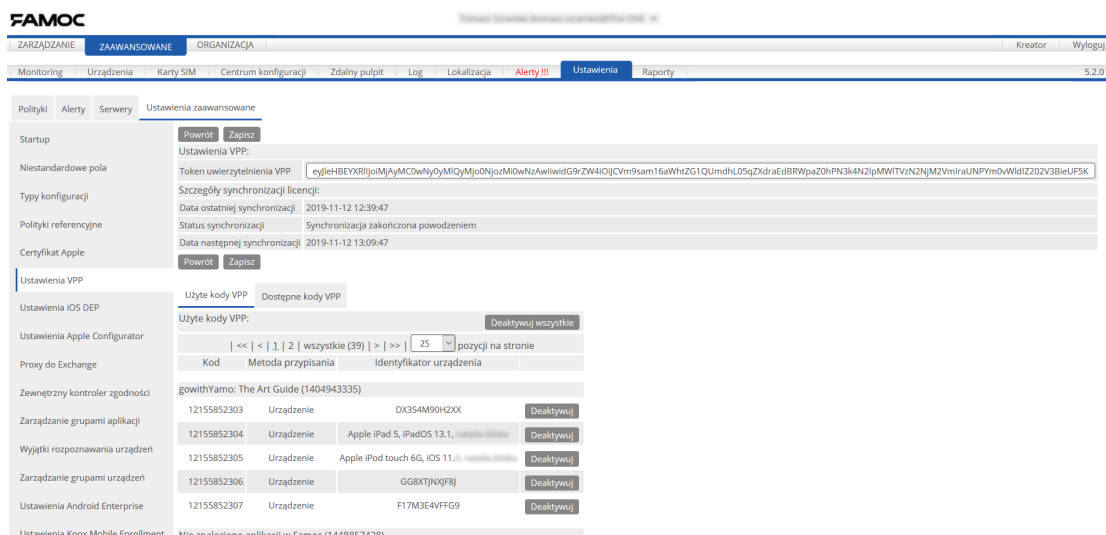
The screenshot shows the 'Ustawienia zaawansowane' (Advanced Settings) section for 'Certyfikat Apple' (Apple Certificate). The interface includes a sidebar with navigation options like 'ZARZĄDZANIE', 'ZAAWANSOWANE', and 'ORGANIZACJA'. The main content area shows fields for editing certificate data, including 'Certyfikat' (Certificate), 'Pobierz żądanie certyfikatu' (Download certificate request), 'Temat' (Subject), 'Ważny od' (Valid from), 'Ważny do' (Valid to), 'Adres email użyty do rejestracji' (Email used for registration), and 'Opis' (Description). A 'Pobieranie żądania certyfikatu' (Downloading certificate request) message is displayed at the bottom.

Rysunek 42 Certyfikat Apple

21.4.6 Ustawienia VPP

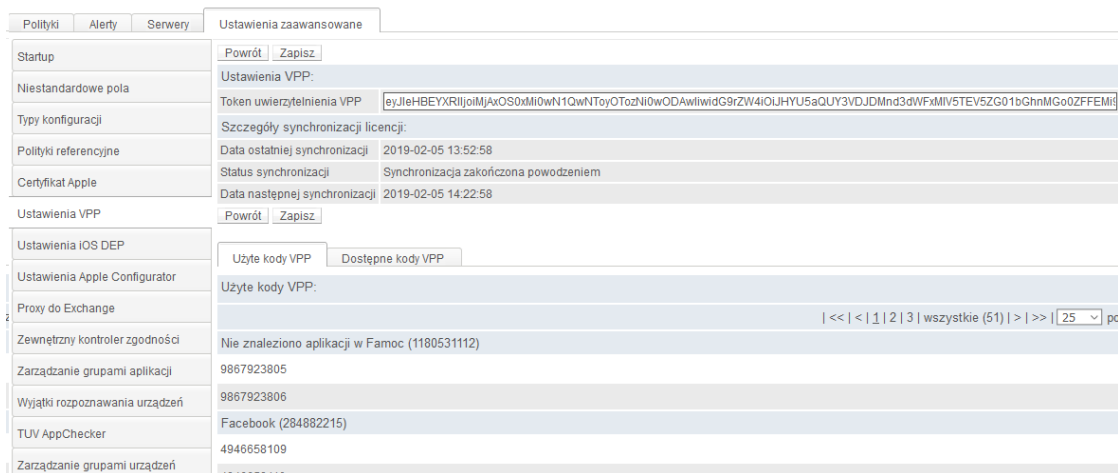
Licencje konta VPP można synchronizować przy użyciu tokena uwierzytelniania. Ustawienia VPP znajdują się w zakładce **ZAAWANSOWANE** → **Ustawienia** → **Ustawienia zaawansowane** → **Ustawienia VPP**.

UWAGA: Program VPP nie jest obecnie dostępny dla firm zarejestrowanych w Polsce.



Rysunek 43 Ustawienia VPP

1. Generuj token na swoim koncie VPP.
2. Wklej token w zakładce Ustawienia VPP systemu FAMOC.
3. Naciśnij Zapisz.
4. Lista dostępnych/wykorzystanych kodów VPP widoczna jest po synchronizacji.
5. W systemie FAMOC możliwe jest zarządzanie i dezaktywacja kodów VPP.



Rysunek 44 Token VPP

21.4.7 Ustawienia iOS DEP

Synchronizacja z programem Apple Device Enrollment Program umożliwia proste dodanie firmowych urządzeń z systemem iOS do systemu zarządzania MDM.

Konfigurację można przygotować w części **ZAAWANSOWANE** → **Ustawienia** → **Ustawienia zaawansowane** → **Ustawienia iOS DEP**, wykonując następujące kroki:

1. Kliknij Dodaj konto.
2. Generuj klucz publiczny/prywatny.
3. Pobierz klucz publiczny.
4. Stwórz wirtualny serwer MDM na stronie <https://deploy.apple.com> i załaduj klucz publiczny.

Uwaga: wymagana jest nazwa pliku klucza publicznego: PublicKey.pem.

5. Załaduj token serwera FAMOC w ustawieniach iOS DEP systemu FAMOC.
6. Przypisz urządzenia do wirtualnego serwera MDM na portalu Apple.
7. W ustawieniach konta iOS DEP wybierz domyślnego użytkownika urządzenia.
8. Ustaw interwał synchronizacji urządzenia.
9. Wykonaj konfigurację setupu urządzenia i naciśnij przycisk Zapisz.
10. Po zapisaniu konfiguracji naciśnij przycisk Rozpocznij synchronizację początkową, aby zsynchronizować wszystkie urządzenia aktualnie przypisane do wirtualnego serwera MDM. Synchronizacja urządzeń z systemem FAMOC jest wykonywana zgodnie z planem.
11. Przycisk **Rozpocznij synchronizację początkową** został teraz zastąpiony przyciskami **Wymuś synchronizację**, **Zatrzymaj synchronizację** i **Zrestartuj synchronizację**, aby kontrolować synchronizację urządzenia.

Rysunek 45 Ustawienia konta iOS DEP

Konfiguracja ustawień startowych

Włącz tryb nadzorowany na urządzeniach

Możliwość włączenia trybu nadzorowanego na urządzeniach. Tryb nadzorowany włącza dodatkowe funkcje MDM na iOS.

Wyłącz usuwanie MDM przy użyciu interfejsu użytkownika na urządzeniu

Jeśli jest zaznaczone, profil MDM nie może zostać usunięty przez użytkownika. Opcja dostępna tylko po włączeniu opcji "Włącz tryb nadzorowany na urządzeniach".

Departament

Informacje o profilu MDM: dział.

Numer telefonu wsparcia

Informacje o profilu MDM: Numer telefonu wsparcia

Adres mailowy wsparcia

Informacje o profilu MDM: Adres mailowy wsparcia

Ukryj i wyłącz okienko z hasłem

Możliwość wyłączenia panelu hasła.

Wyłącz usługi lokalizacyjne

Możliwość wyłączenia usług lokalizacyjnych.

Wyłącz przywracanie z kopii zapasowej

Możliwość wyłączenia przywracania urządzenia z kopii zapasowej.

Wyłącz logowanie do Apple ID i iCloud

Możliwość wyłączenia logowania do Apple ID i iCloud.

Pomiń Warunki użytkowania	Możliwość pominięcia panelu Warunki użytkowania
Pomiń konfigurację Touch ID	Możliwość pominięcia panelu konfiguracji Touch ID.
Pomiń konfigurację Apple Pay	Możliwość pominięcia panelu konfiguracji Apple Pay.
Pomiń konfigurację przybliżania	Możliwość pominięcia panelu ustawień przybliżania.
Jeśli panel Przywracanie nie zostanie pominięty, usuń z niego opcję Przenieś z systemu Android	Jeśli jest ustawione, usuwa opcję "Przenieś z Androida" z panelu przywracania.
Wyłącz Siri	Możliwość wyłączenia Siri.
Wyłącz automatyczne wysyłanie informacji diagnostycznych	Możliwość wyłączenia wysyłania informacji diagnostycznych.

Tabela 10 Ustawienia iOS DEP

Więcej informacji na temat programu DEP znajduje się na dedykowanej stronie firmy Apple <http://www.apple.com/business/dep/>

21.4.8 Apple Configurator

W tej sekcji administrator może wygenerować token, który będzie użyty w trakcie dodawania urządzenia z systemem iOS za pomocą narzędzia Apple Configurator.

W celu uzyskania dodatkowych informacji przeczytaj dokument Apple Configurator Enrollment in FAMOC.

22.4.9 Proxy do Exchange

W tej sekcji administrator może skonfigurować serwer FAMOC jako proxy do serwera Exchange.

1. Użyj przycisku Dodaj adres przekierowania.
2. Wybierz odpowiedni Adres zewnętrzny i port. Lista dostępnych adresów i portów może być tworzona i edytowana wyłącznie z poziomu konfiguratora FAMOC.
3. Ważność cache autoryzacji — określa, jak często odświeżać pamięci podręczne związane z bezpieczeństwem (dostępne opcje — (brak limitu czasu lub od 2 minut do 1 godziny)
4. Wpisz Adres przekierowania.
5. Określ Politykę dostępu (zezwól na dostęp dla wszystkich urządzeń lub zarządzanych urządzeń z jedną z wyszczególnionych polityk).
6. Zapisz ustawienia.
Dostępne polityki dostępu, których można używać z głównymi politykami:
 1. Zezwalaj na dostęp dla wszystkich urządzeń dodanych do systemu FAMOC
 2. Zezwalaj na dostęp dla urządzeń zarządzanych w systemie FAMOC
 - a. Zezwalaj na dostęp urządzeniom, których ostatni kontakt był nie dawniej niż...
 - b. Zezwalaj na dostęp dla urządzeń z listy dozwolonych urządzeń
 - c. Blokuj dostęp dla urządzeń jailbreakowanych

- d. Blokuj dostęp dla urządzeń, na których nie zaaplikowano polityki podstawowej
 - e. Blokuj dostęp dla urządzeń, na których zastosowanie restrykcji bezpieczeństwa nie powiodło się
 - f. Blokuj dostęp dla urządzeń zgłaszających alerty
 - g. Zezwalaj na dostęp tylko urządzeniom identyfikacją KNOX
3. Dodatkowa lista uprawnionych identyfikatorów- administrator może zdefiniować listę identyfikatorów, które mogą komunikować się z serwerem proxy EAS, nawet jeśli polityka proxy EAS zezwala tylko na urządzenia zarządzane. (Listę można zdefiniować w sekcji „Dodatkowa lista autoryzowanych identyfikatorów”. Jeżeli w ustawieniach proxy EAS ustawiona jest opcja „Alert o próbie połączenia przez niezarządzane urządzenie” - będzie możliwość dodania identyfikatora zgłaszanego w alercie bezpośrednio do tej listy.)

Możliwe jest zastosowanie kilku polityk jednocześnie.

Przy wyborze polityki umożliwiającej dostęp urządzeniom z dozwolonej listy, istnieje możliwość zdefiniowania dozwolonych identyfikatorów urządzenia (IMEI, UID, numer seryjny, Exchange ID). Identyfikatory mogą być dodane ręcznie - przycisk Dodaj identyfikator, który otwiera popup z polem tekstowym.

Po zapisaniu ustawień FAMOC będzie wykorzystywany jako proxy do serwera Exchange. FAMOC będzie identyfikować urządzenia po numerze IMEI, numerze seryjnym, UID lub identyfikatora Exchange ID. W przypadku wykrycia próby nawiązania połączenia wychodzącej z niezidentyfikowanego urządzenia, FAMOC generuje alert do wszystkich urządzeń przypisanych do użytkownika. Przypisanie Exchange ID to każdego urządzenia może rozwiązać problem.

Przy wyborze polityki blokowania dostępu urządzeniom, które raportują aplikację z blokowanych aplikacji alert przesyłany do serwera FAMOC może być oznaczony jako ignorowany lub rozwiązany, co oznacza, że dostęp do Exchange'a nie będzie blokowany.

Dostępne są dodatkowe ustawienia alertów:

1. Ostrzeżenie o próbie połączenia przez zablokowane urządzenie - jeśli zaznaczone, alerty będą generowane w interfejsie administratora, gdy zablokowane urządzenie spróbuje połączyć się z Exchange.
2. Alarm podczas próby połączenia przez niezarządzane urządzenie - jeśli zaznaczono, alert zostanie wygenerowany w interfejsie administratora, gdy niezarządzane urządzenie spróbuje połączyć się z Exchange.

21.4.10 Zewnętrzny kontroler zgodności.

W tej sekcji administrator może skonfigurować serwer FAMOC jako kontrolera zgodności dla zewnętrznych środowisk takich jak CISCO ISE, Checkpoint i innych.

1. Użyj przycisku Dodaj kontroler zgodności.
2. Wprowadź nazwę oraz wybierz typ kontrolera zgodności z listy.
3. Identyfikator kontrolera zostanie wygenerowany automatycznie.
4. Określ Politykę zgodności.
5. Zapisz ustawienia.

Wybór polityk zgodności:

1. Zezwalaj na dostęp zarządzanym urządzeniom.

2. Zezwalaj na dostęp urządzeniom, których ostatni kontakt był nie dawniej niż...
3. Blokuj dostęp dla urządzeń raportujących jailbreak/zrootowanych
4. Blokuj dostęp dla urządzeń, na których wystąpił wybrany alert

Możliwe jest zastosowanie kilku polityk jednocześnie.

Do konfiguracji CISCO ISE niezbędny jest identyfikator kontrolera zgodności oraz dane użytkownika FAMOC Web service. Więcej informacji dostępnych jest w dokumentacji FAMOC CISCO ISE Integration Guide.

Checkpoint i inne środowiska zewnętrzne, które chcą weryfikować zgodność urządzeń, mogą wykorzystywać FAMOC Web Service – checkDevice (zwraca on informacje o zgodności). Więcej informacji o checkDevice web service dostępne są w dokumentacji FAMOC Web Service APIs guide.

The image shows two screenshots of the FAMOC web interface. The top screenshot is a modal window titled 'Nowy kontroler zgodności' (New Compliance Controller). It contains the following fields and options:

- Nazwa:** A text input field.
- Rodzaj:** A dropdown menu with the text 'Wybierz typ kontrolera ...'.
- Identyfikator:** A text input field.
- Polityka zgodności:** A section with four checkboxes:
 - ☐ Pozwalaj na dostęp zarządzanym urządzeniom
 - ☐ Pozwalaj na dostęp urządzeniom, których ostatni kontakt był nie dawniej niż ...
 - ☐ Blokuj dostęp dla urządzeń raportujących jailbreak
 - ☐ Blokuj dostęp dla urządzeń, na których wystąpił alert

At the bottom of the modal are two buttons: 'Zapisz' (Save) and 'Anuluj' (Cancel).

The bottom screenshot shows the main interface of the FAMOC system. The top navigation bar includes tabs for 'ZARZĄDZANIE', 'ZAAWANSOWANE' (selected), and 'ORGANIZACJA'. Below this is a sub-navigation bar with links: 'Monitoring', 'Urządzenia', 'Karty SIM', 'Centrum konfiguracji', 'Zdalny pulpit', 'Log', 'Lokalizacja', 'Alerty !!!', 'Ustawienia' (selected), and 'Raporty'. The main content area is titled 'Ustawienia zaawansowane' (Advanced Settings) and includes a sidebar with various configuration options like 'Startup', 'Niestandardowe pola', 'Typy konfiguracji', etc. The main panel shows a table of existing compliance controllers with columns for 'Nazwa', 'Rodzaj', 'Identyfikator', and 'Polityka zgodności'. One entry is visible: 'Cisco ISE ECC' with type 'Cisco ISE' and identifier 'ISE153', with the policy 'Pozwalaj na dostęp zarządzanym urządzeniom'.

Rysunek 46 Zewnętrzny kontroler zgodności

21.4.11 Zarządzanie grupami aplikacji

Ta sekcja umożliwia administratorowi tworzenie, usuwanie, edycję nazwy oraz ikony grup aplikacji dostępnych podczas dodawania nowych aplikacji do system FAMOC. Możliwe jest także przeglądanie wszystkich aplikacji zawartych w danej grupie. Podczas usuwania grupy, system zaleca administratorowi przeniesienie wszystkich aplikacji do innej grupy.

21.4.12 Zarządzanie grupami urządzeń

Ta sekcja umożliwia administratorowi tworzenie, usuwanie lub zmiany grup urządzeń. Administrator ma również możliwość przeglądania urządzeń przypisanych do poszczególnych grup.

ZARZĄDZANIE ZAAWANSOWANE ORGANIZACJA

Monitoring Urządzenia Karty SIM Centrum konfiguracji Zdalny pulpit Log Lokalizacja **Alerty !!!** Ustawienia Raporty

Polityki Alerty Serwery Ustawienia zaawansowane

Startup

Niestandardowe pola

Typy konfiguracji

Polityki referencyjne

Certyfikat Apple

Ustawienia VPP

Ustawienia iOS DEP

Ustawienia Apple Configurator

Proxy do Exchange

Zewnętrzny kontroler zgodności

Zarządzanie grupami aplikacji

Wyjątki rozpoznawania urządzeń

Zarządzanie grupami urządzeń

Dodaj grupę urządzeń Importuj grupy urządzeń Usuń zaznaczone

<< | < | 1 | 2 | wszystkie (43) | > | >> | 25 pozycji na stronie

Nazwa Szukaj Wyczyść

☐	Nazwa grupy	Opis grupy	Liczba urządzeń	Ostatnio zmieniona	Akcje
☐	COPE		5	2019-10-22 11:20:22	
☐	Windows - podstawowa		1	2019-10-16 16:38:37	
☐	COBO		1	2019-10-22 10:50:19	
☐	MR devices		0	2015-10-16 14:03:15	
☐	Lenas - dev		0	2014-08-28 11:41:38	
☐	MariuszRGroup		0	2016-12-14 15:25:17	
☐	Only HTC		0	2014-11-27 13:54:18	
☐	michal s5		0	2014-12-16 15:53:25	
☐	LO group		0	2015-05-15 14:59:31	
☐	Marcin Location Batt		0	2016-04-27 13:47:38	

Rysunek 47 Zarządzanie grupami urządzeń

21.4.13 Ustawienia Android Enterprise

Ta sekcja pozwala administratorowi zarejestrować i zsynchronizować zarządzane konto Google Play do użytku z Profilem Praca Android (więcej informacji znajdziesz w "Podręczniku Android Profil Praca").

21.4.14 Ustawienia Knox Mobile Enrollment

W tej sekcji administrator może generować / odnawiać apk Agentu bazowego dla Knox Mobile Recorder. Możliwe jest także wyeksportowanie listy urządzeń potrzebnych do aktywacji KME. Aby uzyskać więcej informacji, zapoznaj się z dokumentacją KME.

ZARZĄDZANIE ZAAWANSOWANE ORGANIZACJA

Monitoring Urządzenia Karty SIM Centrum konfiguracji Zdalny pulpit Log Lokalizacja **Alerty !!!** Ustawienia Raporty 5.2

Polityki Alerty Serwery Ustawienia zaawansowane

Startup

Niestandardowe pola

Typy konfiguracji

Polityki referencyjne

Certyfikat Apple

Ustawienia VPP

Ustawienia iOS DEP

Ustawienia Apple Configurator

Proxy do Exchange

Zewnętrzny kontroler zgodności

Zarządzanie grupami aplikacji

Wyjątki rozpoznawania urządzeń

Zarządzanie grupami urządzeń

Ustawienia Android Enterprise

Ustawienia Knox Mobile Enrollment

URI serwera MDM

Link do apk agenta MDM

Niestandardowe dane JSON

Opcje

rel-test.fancyfon.com rel-test.fancyfon.com/kme/index.php/HI66zGTCM3QdZHNPEHh0KQuTbPYw5nJ Nie wymagany. Exportuj listę urządzeń

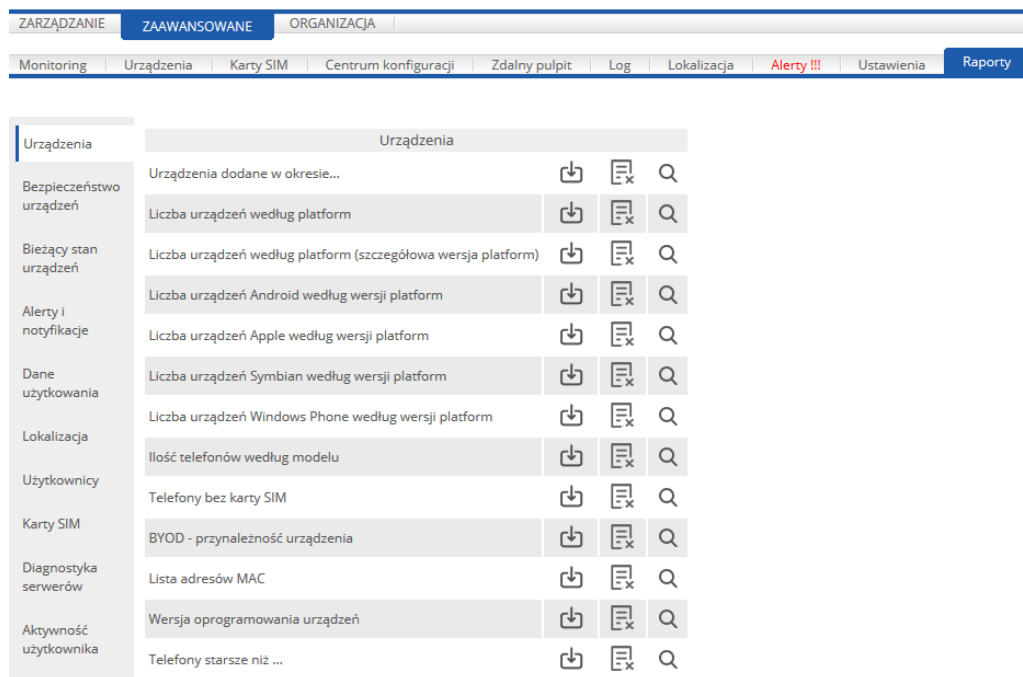
Rysunek 48 Ustawienia Knox Mobile Enrollment

22. Raporty

Raporty służą do gromadzenia danych i statystyk dotyczących FAMOC, urządzeń i użytkowników uwzględnionych w systemie oraz wykonywanych operacji.

22.1 Raporty FAMOC

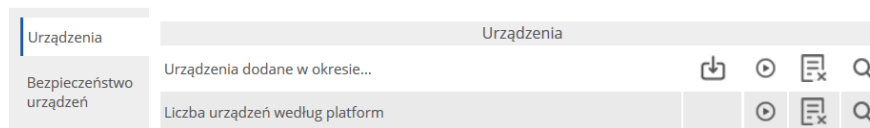
Zakładka Raporty udostępnia statystyki na temat urządzeń, ich bezpieczeństwa i aktualnego stanu, alertów i powiadomień, kart SIM, użytkowników, rozliczeń, diagnostyki serwerów i aktywności użytkowników.



Rysunek 49 Raporty

22.2 Możliwe operacje dostępne w zakładce Raporty

Aby zobaczyć raport, należy kliknąć ikonę Wykonaj na liście raportów. Jeśli dany raport wymaga wyboru parametrów, wyświetla się popup z polami do wypełnienia (np. Data zakończenia). Po wygenerowaniu raportu, pojawi się dodatkowa ikona pozwalająca na pobranie ostatniego raportu.



Rysunek 50 Operacje na raportach

Możliwe jest tworzenie harmonogramów raportów i wysyłanie ich do wybranych odbiorców pocztą e-mail. W tym celu należy kliknąć ikonę Dodaj harmonogram. W oknie Tworzenie harmonogramu należy określić następujące parametry:

1. Interwał harmonogramu – jak często raport ma być tworzony (codziennie, w dni powszednie, raz w tygodniu, co miesiąc).
2. Data początkowa – czas i data wysłania raportu po raz pierwszy

3. Adresaci harmonogramu – lista adresów e-mail oddzielonych średnikiem
4. Aktywuj harmonogram – czy harmonogram ma być aktywny od razu po zapisaniu
5. Parametry raportu – ta część wyświetla się, gdy w raporcie generowane są parametry
6. Ustawienia wiadomości – ta część zawiera pola wymagane takie jak: od, odpowiedz do, tytuł, treść wiadomości. Możliwe jest ustawienie własnych wartości. W polu z tematem nazwę raportu zastąpi token `_REPORT_NAME_`.

Tworzenie harmonogramu: Telefony bez karty SIM

Ustawienia harmonogramu:

Wybierz interwał harmonogramu: --Wybierz--
Data początkowa: 2019-11-12 o godzinie 13:00
Adresaci harmonogramu: Lista adresów email oddzielona średnikiem
Przykład: imie.nazwisko@domena.com; imie2.nazwisko2@domena.com
Aktywuj harmonogram: ☒

Ustawienia wiadomości

Od (nazwa): FAMOC Server
Od (email): famoc-server@venice.l.fancyfon.com
Odpowiedz do (email): famoc-server@venice.l.fancyfon.com
Tytuł: [FAMOC REPORT] _REPORT_NAME_
Treść wiadomości email: Raport w załączeniu.
Stopka wiadomości:

Zapisz Anuluj

Rysunek 51 Tworzenie harmonogramu raportu

23. Dodatkowe informacje

Aby uzyskać wsparcie lub pomoc techniczną, należy skontaktować się z działem wsparcia FAMOC pod adresem support@famoc.com.

Więcej informacji o systemie FAMOC i firmie Famoc znajduje się na stronie www.famoc.pl.