50 PYTAŃ (D)O FAMOCA,

CZYLI ZESTAW NAJCZĘSTSZYCH PYTAŃ O FAMOC MANAGE

Przygotowane przez:
Famoc S.A.

FAMOC manage daje możliwość m.in. dokładnej konfiguracji polityk bezpieczeństwa, wymuszania haseł, geolokalizacji urządzenia czy chociażby zdalnego usuwania danych zgromadzonych na smartfonie.

BARTOSZ LEOSZEWSKI
CEO, Famoc

#ObsessedWithSecurity

FAMOC manage ułatwia wdrażanie, konfigurowanie i zarządzanie wszystkimi smartfonami i tabletami w Twojej organizacji. To jeden system, w ramach którego możesz kontrolować wszystko, czego potrzebujesz: tworzenie profili, zarządzanie ograniczeniami, ustawianie zasad dotyczących PIN i haseł oraz wiele innych.

Niezależnie, czy chcesz zarządzać dziesięcioma czy dziesięcioma tysiącami urządzeń, czy należą one do firmy czy są w modelu BYOD – rejestracja urządzeń jest szybka, łatwa i intuicyjna. FAMOC manage umożliwia wykonywanie działań na jednym telefonie, ale również pozwala na operacje masowe na grupach urządzeń o zróżnicowanych systemach operacyjnych.

Czym jest FAMOC manage?

1. Czy FAMOC manage obsługuje jedynie urządzenia z Androidem?

FAMOC manage obsługuje wszystkie systemy operacyjne - Android, iOS, Windows, macOS*.

2. Jakie są możliwości dodania urządzenia do systemu FAMOC manage?

Urządzenia można dodać do systemu FAMOC manage w sposób ręczny lub zautomatyzowany. Najprostszym sposobem ręcznego enrollmentu jest zeskanowanie kodu QR (dostęp do QR Reader można łatwo uzyskać dotykając sześciokrotnie ekran powitalny na zresetowanym/ nowym urządzeniu). Urządzenie możemy dodać również wykorzystując funkcję NFC (wymaga to dodatkowego urządzenia z aktywną komunikacją NFC, które jest już zarejestrowane w FAMOC) albo za pomocą linku aktywacyjnego, wysłanego na adres e-mail użytkownika lub SMS-em.

Proces ten można zautomatyzować poprzez usługi tzw. autoenrollmentu, które zdalnie instalują i konfigurują agenta MDM po pierwszym uruchomieniu urządzenia i podłączeniu do sieci Internet. Więcej informacji na temat dodawania urządzeń możesz znaleźć **tutaj.**

**Chcesz otrzymać komplet funkcjonalności dla konkretnych wersji systemu? Zgłoś się po naszą matrycę funkcjonalności!*

3. Jakie dane urządzenia wyświetlają nam się w konsoli?

Podstawowe informacje to m.in.: nazwa, model oraz producent urządzenia, jego numer seryjny, numery ID (w tym np. numer telefonu, IMEI, IMSI (ICCID) czy numer wydrukowany na karcie SIM (ID)), przypisany użytkownik. Możemy również monitorować wykorzystanie pamięci, połączenia WiFi, danych roamingu czy nieznanych źródeł (innych niż np. sklep Google Play) itp.

4. Co definiuje ilość urządzeń możliwych do dodania w konsoli?

System pozwala na pełne zarządzanie określoną w licencji ilością urządzeń. Każdy rekord na liście urządzeń to jedna licencja, ważna przez określony okres czasu.

5. Czy dostęp do konsoli administracyjnej może mieć wielu użytkowników?

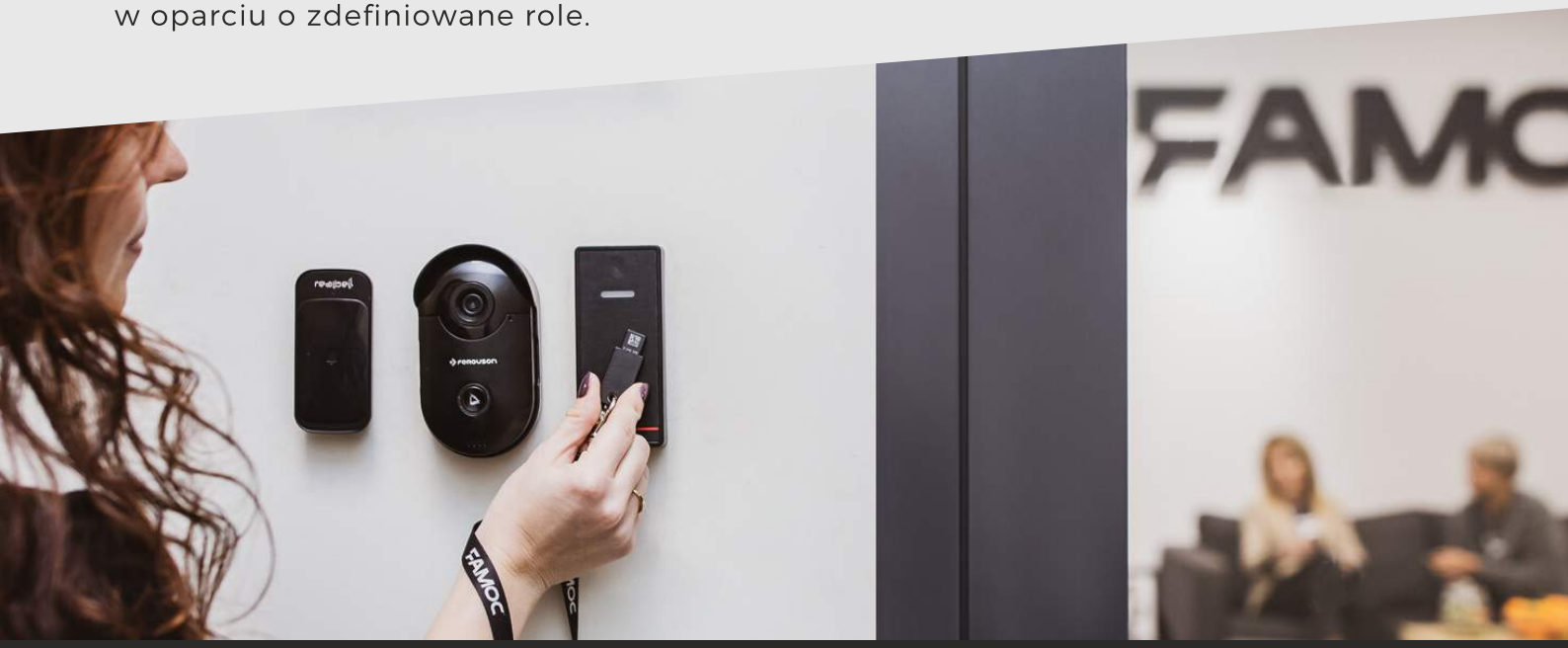
Tak, możliwość dostępu do konsoli administracyjnej systemu FAMOC manage może mieć wielu użytkowników, z podziałem na uprawnienia dostępu do poszczególnych funkcjonalności, w oparciu o zdefiniowane role.

6. Jakie role użytkowników dostępne są w konsoli? Czy można zdefiniować swoje własne?

W konsoli dostępnych jest kilka predefiniowanych ról: Administrator systemu FAMOC, FAMOC Web Services, Menedżer grup FAMOC, Zarządzanie grupami urządzeń lub użytkowników, Menedżer bezpieczeństwa FAMOC, Menedżer zasobów FAMOC. Dodatkowo oczywiście można stworzyć swoje własne.

7. Jaki model wdrożenia systemu FAMOC manage jest możliwy?

Oferujemy dostępność systemu zarówno w modelu instalacji w środowisku wewnętrznym oraz jako rozwiązanie hostowane. Hosting odbywa się na serwerach firmy OVH. Ta opcja instalacyjna wybierana jest częściej przez mniejsze firmy (mniejsza ilość urządzeń), nieposiadające rozbudowanego działu IT, lub w przypadkach, w których klientowi zależy na szybkim uruchomieniu usługi. Minimalny okres licencji w środowisku hostowanym to 12 miesięcy. Nie ma minimalnej liczby urządzeń.



System FAMOC może być również instalowany na serwerze fizycznym klienta, zlokalizowanym w siedzibie klienta lub w oparciu o środowisko VMWare klienta. W obu przypadkach zapewniane jest wsparcie w zakresie instalacji, integracji oraz konfiguracji. Ta opcja instalacyjna wybierana jest częściej przez większe firmy, zarządzające dużą ilością urządzeń mobilnych, posiadające rozbudowany dział IT. Firmom tym zależy na pełnej kontroli nad zarządzaną flotą urządzeń mobilnych. Licencja on-site jest bezterminowa.

Opcjonalnie można zdecydować się na hosting dedykowany - w chmurze, ale na osobnym serwerze.

8. Czy FAMOC manage obejmuje funkcję zdalnego dostępu/ zdalnego pulpitu? Czy jest ona dodatkowo płatna?

Usługa zdalnego dostępu jest dostępna dla wszystkich użytkowników systemu FAMOC manage i nie jest funkcją dodatkowo płatną. Zdalny pulpit jest w standardzie rozwiązania FAMOC manage. Więcej informacji o zdalnym dostępie znajdziesz **tutaj**.

9. Czym różni się wersja FAMOC manage standard od FAMOC manage enterprise?

Obie wersje bazują na tej samej konsoli FAMOC. Wersja enterprise posiada jednak rozszerzony zakres funkcjonalności, m.in. dostępność API, zarządzanie rozszerzone o urządzenia działające na systemie operacyjnym Windows 8 (i nowsze) oraz Mac, dedykowane rozwiązanie VPN (FAMOC manage tunnel) i inne. Kompletne porównanie obu wersji znajdziesz na **support.famoc.com**.

10. Czym jest rozwiązanie FAMOC lock?

Rozwiązanie FAMOC lock bazuje na systemie FAMOC manage. Elementem FAMOC lock jest aplikacja, która nie może zostać usunięta. Celem jest ochrona i kontrola urządzeń zakupionych na raty i spłacanych przez użytkownika końcowego. W przypadku zaległych opłat, aplikacja wyświetla użytkownikowi notyfikację o braku płatności, która przez określony okres czasu (np. kilka minut) nie może zostać zminimalizowana ani zamknięta. Jeśli użytkownik wciąż zalega z płatnością, urządzenie może zostać zdalnie zablokowane.

11. Czym jest rozwiązanie FAMOC defend?

Rozwiązanie FAMOC defend również bazuje na systemie FAMOC manage. Ponieważ rozwiązanie to kierowane jest głównie dla sektora rządowego, priorytetem w tym wypadku są skomplikowane wymagania związane z ochroną danych. Dzięki FAMOC defend instytucje państwowe otrzymują wsparcie już pierwszego dnia dla wszystkich systemów operacyjnych, mogą kontrolować sposób szyfrowania komunikacji oraz zarządzać dostępem do sieci ze zdalnych urządzeń. Jest to rozwiązanie 'szyte na miarę' zgodnie z potrzebami danej organizacji.

12. Czy rozwiązanie FAMOC manage integruje się z systemami autentykacji SSO?

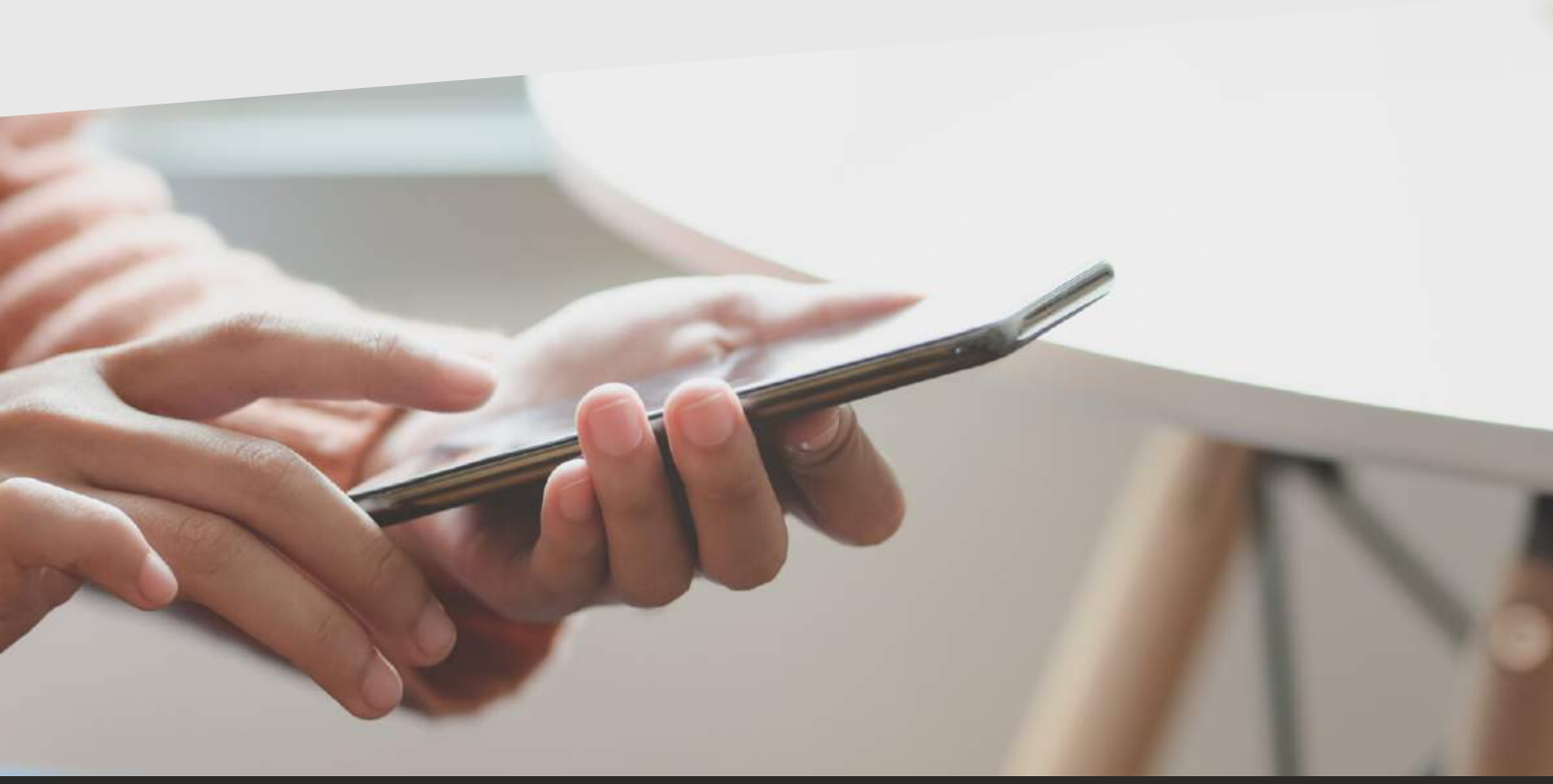
Tak, FAMOC manage ma możliwość integracji z systemem autentykacji i autoryzacji SSO - Microsoft Active Directory, oraz rozwiązaniami bazującymi na protokole SAML, tj. Azure Active Directory, Swivel Secure czy Okta.

13. Czy możliwa jest integracja systemu FAMOC manage z serwerem pocztowym MS Exchange?

Naturalnie, FAMOC manage jest zintegrowany z serwerem pocztowym Microsoft Exchange i obsługuje uwierzytelnianie do serwera Microsoft Exchange przy użyciu certyfikatu - klucza prywatnego.

14. Moja organizacja wymaga tworzenia raportów o zarządzanych urządzeniach. Czy można takie raporty generować w konsoli FAMOC manage?

Oczywiście, możemy tworzyć cykliczne raporty danych o zarządzanych urządzeniach. Raporty mogą zawierać m.in takie informacje, jak: typ i model urządzenia, wersja systemu operacyjnego zainstalowanego na urządzeniu, lista zainstalowanych aplikacji wraz z ich wersją, ilość zajętej i wolnej pamięci, numer seryjny karty SIM etc.



15. W jakich językach dostępne jest wsparcie w ramach platformy FAMOC?

Języki dostępne w obrębie samej platformy to polski, angielski i hiszpański. Dodatkowo, w związku z rozbudowaną siecią partnerską, możemy zaoferować wsparcie w języku rosyjskim i niemieckim.

16. Gdzie znajdę dokumentację systemu?

Dokumentacja FAMOC, w języku polskim i angielskim, dostępna jest na **support.famoc.com** - zawiera ona opisy i instrukcje, przeznaczone zarówno dla użytkownika, ale też administratora systemu. Przykładowe instrukcje znajdziesz pod linkami: **Famoc Admin Guide**, **Szablony polityk**, **Dodawanie urządzeń**, **Android Enterprise**.

17. Czy licencje są przypisane per urządzenie czy per użytkownik?

Licencja jest generowana na określoną liczbę urządzeń oraz czas (lub licencja wieczysta). Po usunięciu dowolnego urządzenia istnieje możliwość jej powtórnego wykorzystania w celu rejestracji nowego urządzenia.

18. Czy możemy dowolnie definiować sobie widok listy zarejestrowanych urządzeń?

Tak, widok listy zarejestrowanych urządzeń mobilnych w konsoli administracyjnej może być modyfikowany, np. w zakresie następujących atrybutów: model urządzenia, numer IMEI urządzenia, imię i nazwisko użytkownika, system operacyjny itp.

19. Czy oferujecie szkolenia związane z administrowaniem bądź utrzymaniem systemu FAMOC manage?

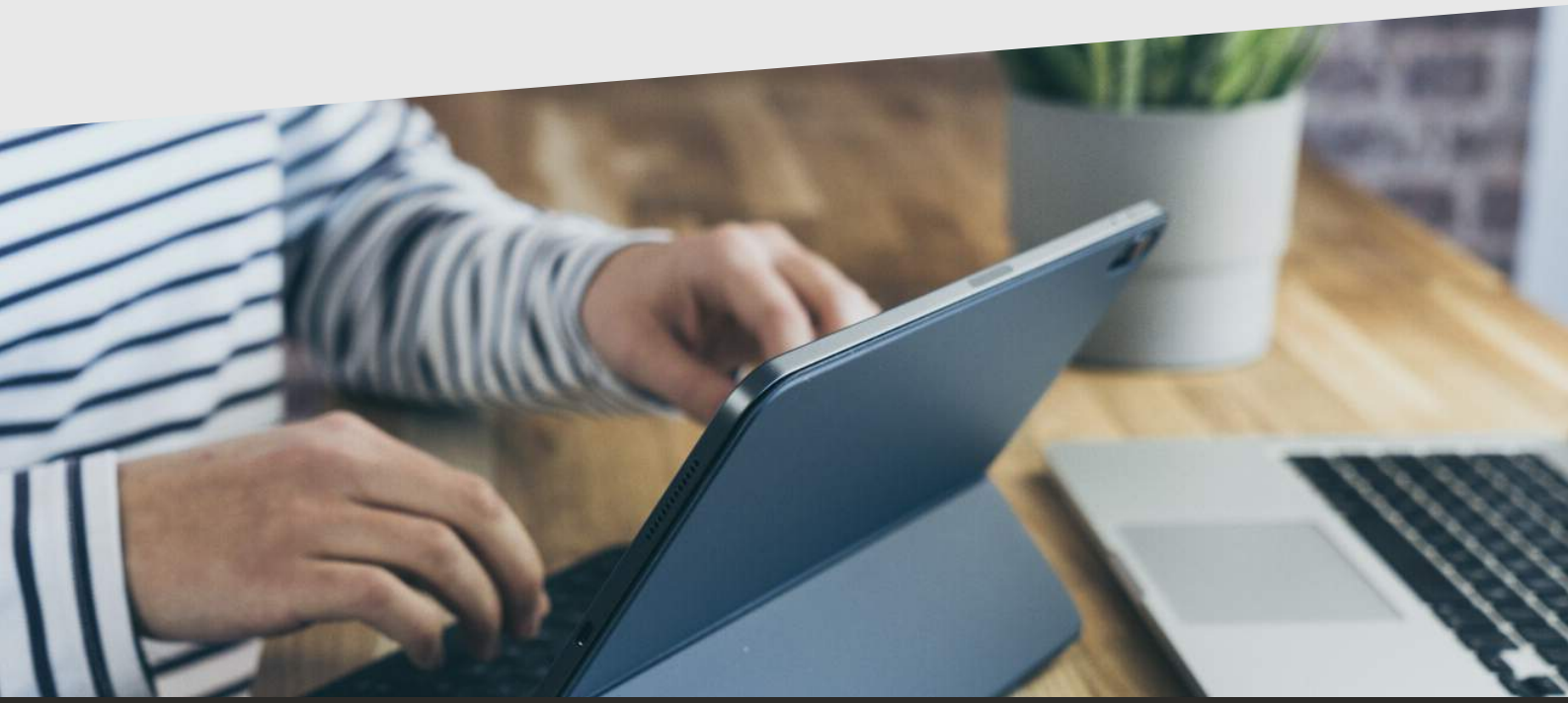
Tak, oferujemy szkolenia w różnych wariantach, w zależności od potrzeb. Wykonujemy szkolenia dla administratorów, gdzie uczestnicy uczą się, jak samodzielnie zarządzać urządzeniami w systemie FAMOC manage. Szkolimy również osoby świadczące helpdesk, gdzie uczestnicy z działu pomocy technicznej poznają mechanizmy działania systemu FAMOC manage oraz sposoby rozwiązywania potencjalnych problemów u użytkowników końcowych. Wspieramy również działy utrzymania poprzez szkolenia dedykowane dla wdrożeń on-site. Podczas tych szkoleń uczestnicy zdobywają podstawową wiedzę o zarządzaniu i administracji FAMOC manage, ale przede wszystkim uczą się, jak sprawnie poruszać się po samym serwerze FAMOC manage, bazie danych, logach oraz narzędziach konfiguracyjnych.

20. Czy rozwiązanie FAMOC manage jest wśród rozwiązań Android Enterprise Recommended?

Aktualnie spełniamy wymagania Advanced Management Set zarówno dla Work Profile, jak i Full Device management. Następny krok to oczywiście Recommended, nad którym obecnie intensywnie pracujemy. Nasz status można sprawdzić **tutaj**.

21. Jakie informacje w zakresie monitorowania lokalizacji są dostępne w systemie FAMOC manage?

Zakładka Lokalizacje pozwala na monitorowanie lokalizacji urządzenia lub użytkownika, ustalonej na podstawie danych pobranych z urządzenia mobilnego. Administrator może zobaczyć na mapie ostatnią pozycję każdego urządzenia, z którego pobrane zostały dane o lokalizacji. Wszystkie wyświetlone na liście urządzenia mogą zostać posortowane za pomocą odpowiednich kolumn poprzez kliknięcie w wybraną nazwę. Dla każdego urządzenia dostępny jest wgląd do ostatnio pobranej pozycji na mapie oraz 20 poprzednich lokalizacji urządzenia.



#Bezpieczeństwo

22. Jakie restrykcje bezpieczeństwa możemy wymusić na użytkowniku?

Możliwości takich konfiguracji jest sporo: od wymuszenia odpowiedniej blokady urządzenia (np. 6-cyfrowy kod PIN), poprzez ograniczenia związane z korzystaniem z dostępnych sieci Wi-Fi, restrykcje dotyczące dostępności i korzystania z aplikacji, przeglądarki internetowej, po możliwość wyczyszczenia bądź zablokowania urządzenia w przypadku kradzieży lub zgubienia. Podobne przykłady można mnożyć.

23. Czy restrykcje bezpieczeństwa mogą być różne dla różnych użytkowników/ grup użytkowników?

Tak. W zależności od potrzeb, istnieje możliwość stworzenia wielu polityk/ profili bezpieczeństwa dla różnych grup użytkowników oraz grup urządzeń.

24. Czy możemy wymusić specjalne restrykcje dotyczące haseł na urządzeniu?

Zdecydowanie. W tym zakresie możemy m.in. zdefiniować wymóg wpisywania hasła przy uruchamianiu urządzenia, zdefiniować stopień skomplikowania hasła (wymóg cyfr, znaków specjalnych), ale też czas bezczynności, po którym następuje automatyczna blokada wymuszająca ponowne wpisanie hasła oraz maksymalna ilość prób jego wpisania, po których następuje usunięcie danych z urządzenia.

25. Co możemy zrobić w przypadku zgubienia lub kradzieży telefonu?

Przede wszystkim możemy zlokalizować urządzenie. Oczywiście możemy również zdalnie usunąć dane z urządzenia w przypadku jego utraty, możemy zdalnie zablokować urządzenie oraz wyświetlić komunikat do “znalazcy”, w przypadku takiej blokady.

26. Jakie opcje blokowania korzystania z Wi-Fi dostępne są w systemie FAMOC manage?

FAMOC manage udostępnia następujące opcje kontroli Wi-Fi: blokada interfejsu Wi-Fi, blokada automatycznego łączenia do punktów dostępowych Wi-Fi, blokada raportowania punktów dostępowych Wi-Fi oraz blokada ręcznej konfiguracji Wi-Fi.

27. Czy FAMOC manage może być odinstalowany na urządzeniu?

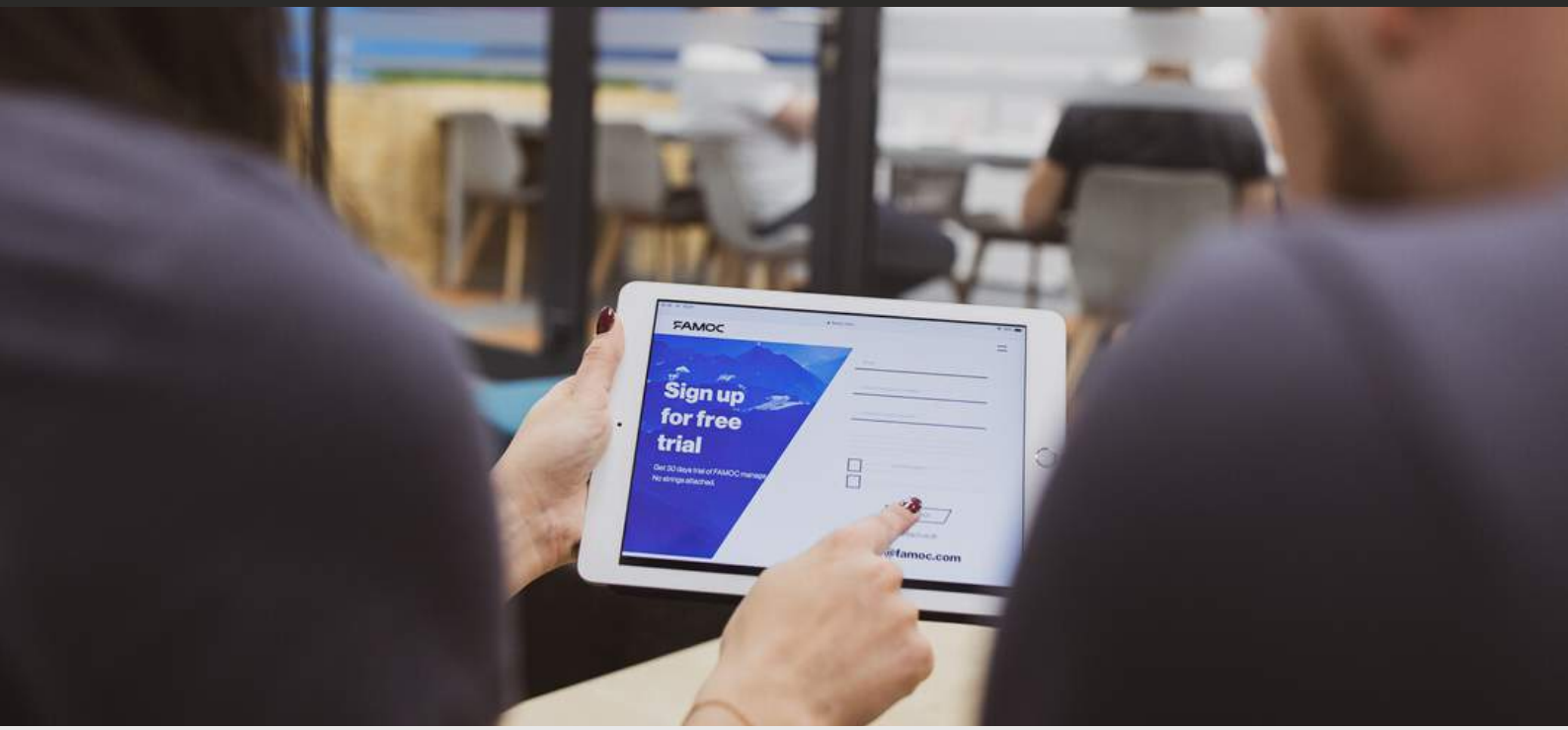
Jeżeli urządzenie jest skonfigurowane w trybie Device Owner, nie ma możliwości usunięcia aplikacji FAMOC (jest możliwa jedynie opcja wipe). Kiedy urządzenie dostępne jest w trybie BYOD, istnieje możliwość ręcznego usunięcia zarządzania.

28. Czy jest możliwa opcja konfiguracji urządzenia, tak aby blokowało się po włożeniu obcej karty SIM?

Tak, możliwa jest blokada urządzenia w przypadku zmiany karty SIM, z jednoczesnym powiadomieniem administratora.

29. Dlaczego FAMOC manage wymaga przestarzałego i dość dziurawego rozwiązania FLASH?

W przeszłości nasze rozwiązanie do zdalnego pulpitu oparte było właśnie na technologii flash (zakładka Remote Access w Advanced UI). Aktualnie zostało zastąpione przez nowszą technologię i nowoczesne rozwiązanie oparte na HTML5.



30. Czy jest możliwe zablokowanie wybranych funkcji w telefonie, np. aparatu fotograficznego?

Tak, istnieje możliwość zablokowania niektórych funkcji telefonu (np. kamera, przeglądarka internetowa, łączność bluetooth itd.). Dowiedz się więcej **tutaj**.

31. Jakie dostępy możemy zablokować użytkownikowi w ramach kontenera?

Możemy m.in. zablokować dostęp do przeglądarki internetowej, do konfiguracji konta e-mail czy do opcji ustawień w kontenerze. Możemy również np. zablokować udostępnianie danych poza środowisko kontenera itd.

#Konfiguracje

32. Czy zdalna konfiguracja urządzeń (w tym np. instalacja aplikacji) może obejmować jedynie określoną grupę urządzeń?

Tak, wszelkie akcje wykonywane na telefonach (m.in. instalacja aplikacji, konfiguracja, wykonanie kopii zapasowej danych) mogą być wykonywane na pojedynczym urządzeniu, na wszystkich urządzeniach jednocześnie lub na określonej grupie (lub wielu grupach) urządzeń - z poziomu konsoli administracyjnej systemu.

33. Czy w ramach konfiguracji poczty e-mail na smartfonach, możliwa jest konfiguracja aplikacji firm trzecich?

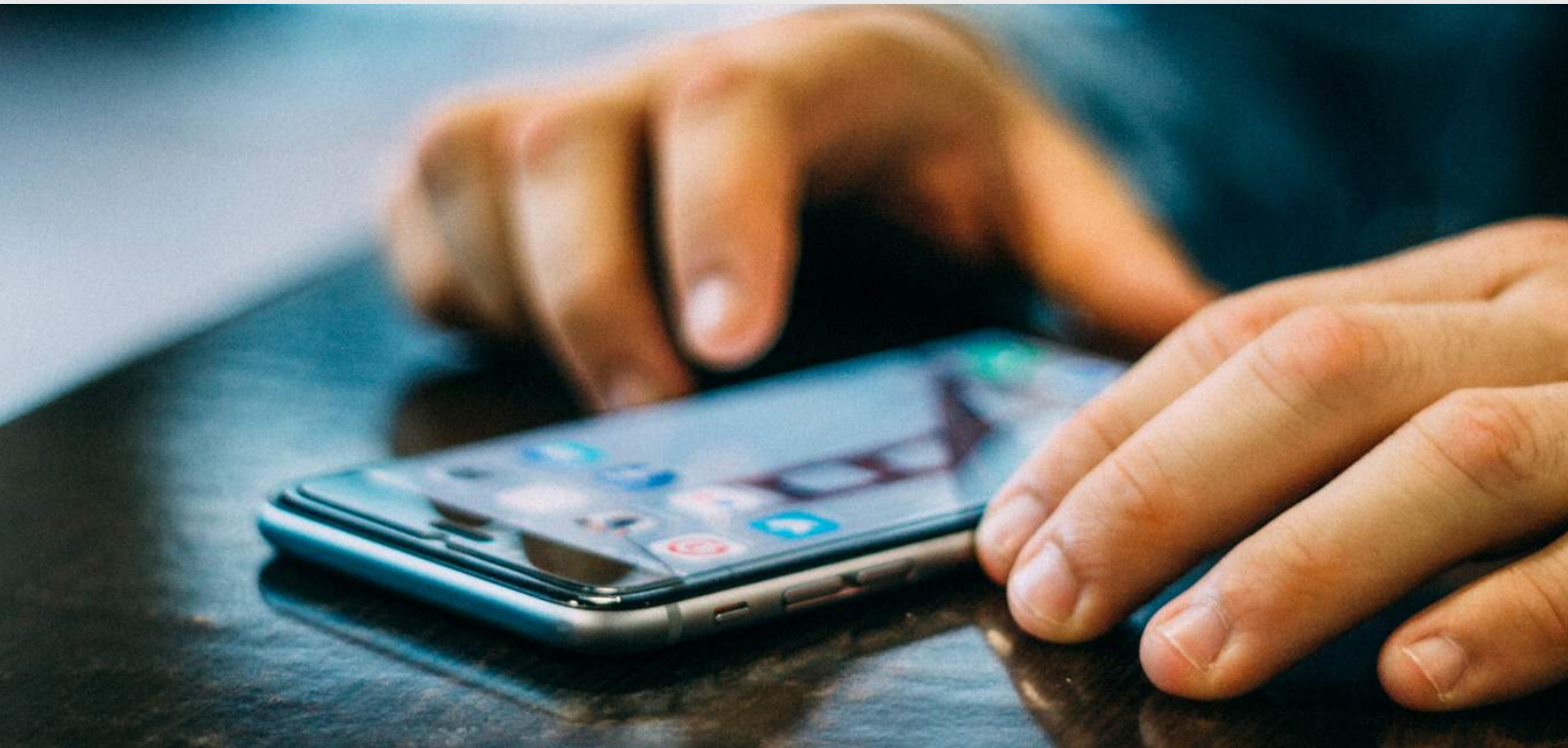
Tak, istnieje możliwość instalacji oraz konfiguracji aplikacji firm trzecich, a także możliwość konfiguracji aplikacji wewnętrznych klienta, poprzez dedykowaną integrację z systemami bazodanowymi klienta.

34. Jakie są możliwości "moderacji" aplikacji na urządzeniach służbowych?

FAMOC manage umożliwia stworzenie białej listy (dozwolonych) aplikacji oraz czarnej listy (aplikacje niedozwolone), a także ciche usuwanie niepożądanych aplikacji z urządzeń. Możemy również skonfigurować wewnętrzny sklep z aplikacjami “corporate appstore”.

35. W jakim trybie możliwe jest odpytywanie lokalizacji urządzenia?

Możliwe jest zarówno odpytywanie o lokalizację w trybie na żądanie, ale również odpytywanie o lokalizację w trybie ciągłym, z możliwością zdefiniowania interwałów (np. w zależności od zmiany lokalizacji o konkretną odległość, zmiany interwału czasowego czy też zmiany ID stacji bazowej, w której znajduje się telefon komórkowy).



36. Jakie ograniczenia profilu służbowego może skonfigurować administrator?

Przykładowe z nich to: blokada przechwytywania obrazu (aby zapobiec udostępnianiu danych), blokada aparatu, blokada możliwości kopiuj-wklej, blokada przenoszenia plików między profilami i inne.

37. Czym jest sklep firmowy z aplikacjami?

Zakładka Sklep firmowy umożliwia dodawanie do systemu sprofilowanych sklepów z aplikacjami i przypisywanie do nich odpowiednich grup użytkowników. Administrator ma również możliwość wglądu w dany sklep (listę dostępnych aplikacji podzielonych na grupy) i jego ustawienia. Może też edytować i usuwać sklepy z repozytorium.

38. Czy jest możliwa konfiguracja urządzenia, tak aby spełniało jedną konkretną funkcję (np. działanie tylko jednej aplikacji)?

Tak, taką możliwość daje tzw. tryb kioskowy (uruchomiona jedna aplikacja na urządzeniu przenośnym, bez możliwości jej wyłączenia). Przeczytaj więcej o trybie kiosk oraz opcji FAMOC Launcher **tutaj**.

39. Czy możemy podejrzeć listę zainstalowanych aplikacji na urządzeniu oraz szczegóły dot. tych aplikacji?

Tak, możemy mieć wgląd do listy zainstalowanych aplikacji na urządzeniu, a także do szczegółowych informacji dotyczących tych aplikacji (m.in. nazwa i wersja aplikacji).

40. Czy możemy wymusić okresową zmianę hasła na urządzeniu z poziomu konsoli administracyjnej?

Tak, możemy wymusić okresową zmianę hasła na urządzeniu.

41. Co daje integracja kluczy YubiKey z FAMOC manage?

Administrator IT obsługujący platformę FAMOC może zdalnie skonfigurować VPN i użyć fizycznego klucza do połączenia VPN i autoryzacji użytkownika. Pracownik może w łatwy sposób się uwierzytelnić za pomocą prostego dotknięcia NFC i zalogować się do sieci firmowej dzięki kluczowi YubiKey.

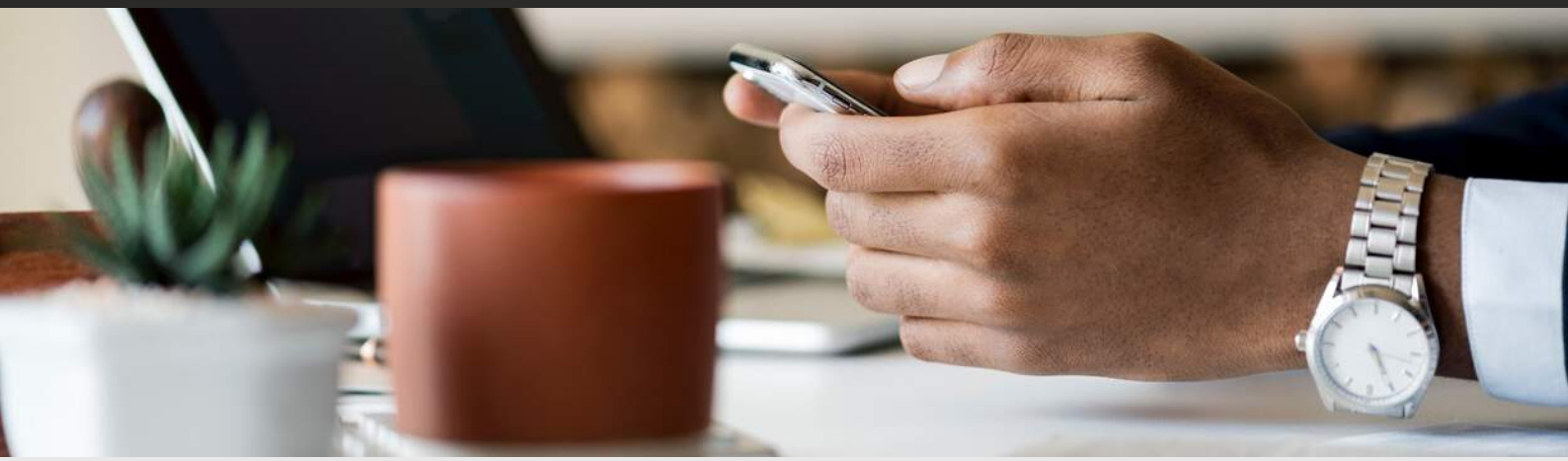
42. Czy z FAMOC manage można skonfigurować klienta VPN na zarządzanych urządzeniach? Jeżeli tak to jakiego dostawcy?

Elementem FAMOC manage jest wbudowana brama VPN, którą można w prosty sposób zdalnie wymusić na zarządzanych urządzeniach. Dodatkowo z poziomu FAMOC manage możliwa jest zdalna konfigruacja klientów VPN czołowych dostawców, takich jak: Cisco Anyconnect, F5, Pulse Secure, Palo Alto, Fortinet i wiele innych.

43. W firmie mamy potrzebę posiadania książki biznesowej zarządzanej centralnie. Czy FAMOC manage oferuje taką funkcjonalność?

Tak, w FAMOC manage jest możliwość włączenia synchronizacji kontaktów użytkowników. Dzięki temu można stworzyć książkę biznesową dedykowaną dla każdego pracownika. Wówczas pracownik otrzyma kontakty do wszystkich pracowników lub wybranych - zależnie od tego, w jakim dziale pracuje.

#Prywatność



44. Czy użytkownik urządzenia musi wyrazić zgodę na przechwycenie jego ekranu i dostępu do urządzenia?

Tak, użytkownik urządzenia musi wyrazić zgodę na zdalny dostęp, czyli autoryzować połączenie.

45. Czy administrator będzie miał dostęp do prywatnych danych (zdjęć, wiadomości) użytkownika?

Nie, nasz system spełnia wymogi Rozporządzenia o Ochronie Danych Osobowych, a prywatność użytkowników jest dla nas kluczowa. Wspieramy konteneryzację danych - nawet jeśli pracownicy wykorzystują swoje prywatne urządzenia do celów prywatnych (BYOD - Bring Your Own Device), zarządzanie danymi służbowymi odbywa się tylko w ramach wyznaczonego kontenera. W takim przypadku Administrator nie ma dostępu do prywatnych danych użytkownika znajdujących się poza częścią służbową.

46. Czy użytkownik może instalować dowolne aplikacje na telefonie służbowym?

To zależy od modelu zarządzania urządzeniami mobilnymi oraz od zakresu uprawnień nadanych przez administratora IT w konkretnej organizacji. W systemie FAMOC manage można skonfigurować białą i czarną listę aplikacji, która będzie dotyczyć całego urządzenia lub jedynie części służbowej.

47. Czy można korzystać z tej samej aplikacji w osobnych profilach (prywatny/ służbowy)?

Tak, w takiej sytuacji należy dokonać osobnej instalacji tej samej aplikacji na oddzielnych profilach.

48. Jeśli w przypadku zagubienia lub kradzieży telefonu, będziemy chcieli wyczyścić dane znajdujące się na urządzeniu - czy możemy to przeprowadzić zachowując dane prywatne użytkownika?

Na urządzeniach, które posiadają oddzielną przestrzeń służbową, zarządzaną przez administratora IT, możliwa jest ingerencja jedynie w dane znajdujące się w tej części urządzenia.

49. Skąd wiadomo, że - w przypadku wykorzystania prywatnych urządzeń użytkowników do celów służbowych (BYOD) - dane służbowe zostaną odpowiednio zabezpieczone?

Kontener służbowy może być zaszyfrowany oraz chroniony dodatkowym hasłem. Możemy też np. zablokować wysyłanie/ kopiowanie treści z przestrzeni służbowej do prywatnej, aby uniemożliwić jej przekazywanie dalej.

50. Czy możemy wyłączyć czasowo profil służbowy?

Tak, może to zrobić użytkownik urządzenia. Profil służbowy można wyłączyć (np. na czas weekendu czy urlopu) - wówczas nie przychodzą do nas żadne powiadomienia, a żeby go z powrotem uaktywnić należy podać hasło blokady.

MASZ WIĘCEJ PYTAŃ? NAPISZ DO NAS:

presales@famoc.com