Aby utrzymać wysokie standardy bezpieczeństwa, czasami konieczne jest wdrożenie bardzo restrykcyjnej polityki bezpieczeństwa. W modelu COBO (Company Owned, Business Only) pracownicy mogą wykorzystywać swoje urządzenia jedynie do celów służbowych i mają niewielkie (lub żadne) możliwości dostosowywania urządzeń. Jest to dość restrykcyjna polityka, jednakże pozwala na ograniczenie ryzyka złamania zabezpieczeń do minimum.

FAMOC udostępnia wiele możliwości zabezpieczenia urządzeń firmowych od potencjalnych niebezpieczeństw takich jak malware czy phishing. W tym artykule przedstawimy kilka sugestii konfiguracji Opcji bezpieczeństwa w FAMOC dla modelu COBO. Aby rozpocząć, zaloguj się do konsoli FAMOC i przejdź do zakładki **ZAAWANSOWANE** > **Ustawienia** > **Polityki**. Następnie **Edytuj** istniejący lub **Dodaj** nowy szablon polityki.

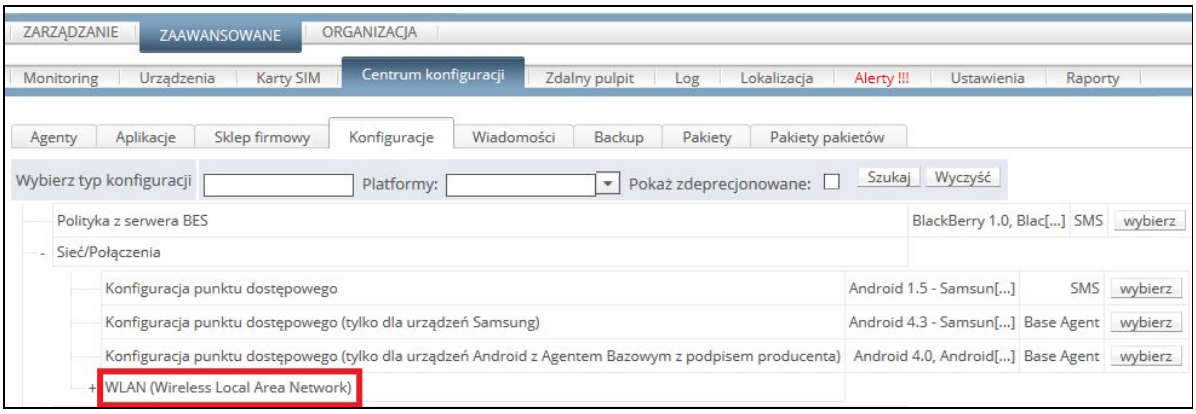
W modelu COBO niezwykle ważne jest aby uniemożliwić użytkownikom zmianę istotnych ustawień oraz aplikacji. Sugerujemy, aby w zakładce **Opcje bezpieczeństwa** zwrócić szczególną uwagę na poniższe elementy.

Polityka czyszczenia danych

Czyszczenie urządzenia po wykryciu rootowania: Po zrootowaniu urządzenia możliwe jest ominięcie zabezpieczeń Androida i uzyskanie dostępu do danych, które byłyby w innym przypadku zabezpieczone. Przechowywanie danych na takim urządzeniu jest ryzykowne, dlatego zalecamy zaznaczenie tej opcji.

Polityka sieci

Blokada ręcznej konfiguracji WiFi: Uniemożliwia ręczną konfigurację połączeń WiFi. Możesz skorzystać z **Konfiguracji**, aby zdefiniować ustawienia WiFi np. dla sieci biurowej.



Blokada danych pakietowych w roamingu: Koszt danych komórkowych w roamingu zależy od kraju, który odwiedzasz. W UE nie powinno to stanowić problemu, ale w innych krajach może generować większe koszty. Możesz rozważyć zablokowanie danych komórkowych w roamingu, aby uniknąć tego problemu.

Blokada udostępniania internetu przez WiFi / USB: Ta opcja blokuje możliwość korzystania z telefonu jako routera lub modemu USB. Zdecydowanie zaleca się używanie prywatnego APN (Access Point

Name) do bezpiecznego połączenia z siecią korporacyjną. W ten sposób tylko autoryzowane urządzenia mają dostęp do infrastruktury sieciowej Twojej firmy. Tworzenie mobilnego punktu dostępowego może stwarzać pewne ryzyko włamania do sieci, zwłaszcza gdy używane są ustawienia domyślne.

Polityka sprzętowa

Blokada aktualizacji OTA: Ta opcja blokuje aktualizację systemu przez 30 dni. Daje to czas na zapewnienie kompatybilności Twoich aplikacji z nową wersją systemu.
Blokada przywracania ustawień fabrycznych: Aby mieć pewność, że przygotowana w szczegółach konfiguracja nie zostanie usunięta "jednym kliknięciem" zalecamy zaznaczenie tej opcji. Zablokowanie możliwości fabrycznego resetu gwarantuje, że urządzenie będzie działać zgodnie z ustaloną polityką.
Blokada opcji programisty: W trybie programisty użytkownicy uzyskują dostęp do pewnych funkcji niskiego poziomu takich jak np. fałszywa lokalizacja GPS. Aby zachować pełną kontrolę nad urządzeniem, sugerujemy włączenie tej funkcji.
Blokada nieznanych źródeł: W trybie COBO użytkownicy powinni korzystać tylko z zatwierdzonych aplikacji. Instalacja plików .apk z nieznanych źródeł może być ryzykowna i powinna być zablokowana.
Blokada karty pamięci: Wymuszanie tak szerokich środków bezpieczeństwa byłoby bezcelowe, gdyby użytkownik mógł po prostu skopiować dane na kartę pamięci i otworzyć je na innym urządzeniu. Przy obecnych możliwościach przechowywania danych w chmurze, warto rozważyć zablokowanie użycia gniazda kart pamięci.
Blokada trybu przeglądania plików USB: Ta opcja blokuje kolejną możliwość wycieku danych, np. podczas korzystania z publicznych gniazd ładowania. Po jej włączeniu, transfer danych za pomocą kabla USB będzie niemożliwy.
Blokada trybu awaryjnego: Tryb awaryjny jest przydatny do rozwiązywania niektórych problemów z urządzeniem. W trybie COBO zależy nam jednak, aby tylko uprawnione osoby zajmowały się wszelkimi usterkami oraz błędami. Dlatego też sugerujemy blokadę trybu awaryjnego i pozostawienie rozwiązywania problemów w rękach działu IT.

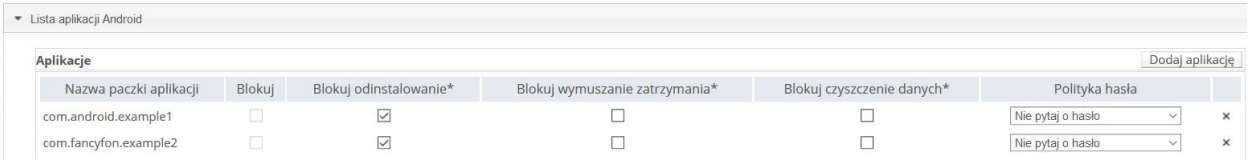
Ograniczenia aplikacji

Wymuś użycie Google Play Protect: Google Play Protect jest skuteczną odpowiedzią na zagrożenia wynikające z aktywności malware'u i innych podejrzanych aplikacji. To zabezpieczenie skanuje Twoje urządzenia każdego dnia w poszukiwaniu niebezpiecznego oprogramowania i pomaga w bezpiecznym korzystaniu z Internetu. Ta opcja aktywuje ochronę Google Play Protect i uniemożliwia jej wyłączenie.
Wyłącz możliwość kontrolowania aplikacji: Uniemożliwia użytkownikom modyfikowanie uprawnień aplikacji, czyszczenie danych lub pamięci podręcznej.
Wyłącz możliwość modyfikowania kont: Użytkownicy będą mogli korzystać na urządzeniu jedynie z predefiniowanych kont. Używanie innych kont będzie zablokowane.

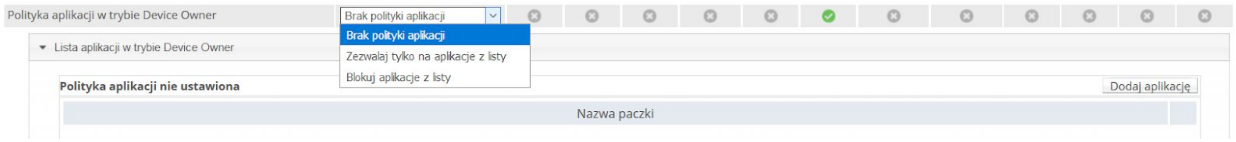
Polityka aplikacji

W tej zakładce można ustawić ograniczenia dla konkretnych aplikacji. W sekcji **Lista aplikacji Android** można dodać aplikacje i zablokować ich instalację używając opcji **Blokuj**. Można również zablokować **odinstalowanie**, **wymuszenie zatrzymania** oraz **czyszczenia danych**. W tym przypadku decyzja odnośnie aplikacji należy do Ciebie. Jeśli pewne aplikacje są niezbędne zalecamy dodanie ich do listy i zaznaczenie opcji **Blokuj odinstalowanie**, aby użytkownicy nie mogli ich usunąć, nawet przypadkowo. Z

drugiej strony, jeśli uważasz, że konkretne aplikacje powinny być zablokowane użyj opcji **Blokuj**, co pozwala na stworzenie “czarnej listy” aplikacji.



W sekcji **Polityka aplikacji w trybie Device Owner** możesz stworzyć listę aplikacji dla trybu Device Owner i z menu rozwijanego powyżej wybrać opcję **Zezwalaj tylko na aplikacje z listy** lub **Blokuj aplikacje z listy**.



Ostatnia sekcja zawiera uprawnienia aplikacji. Po dodaniu aplikacji w zakładce **Globalna polityka uprawnień aplikacji w trybie Device Owner** możesz zdefiniować jej uprawnienia, które nie będą mogły być zmienione przez użytkownika. Jeśli chcesz możesz na przykład zablokować dostęp aplikacji do informacji o lokalizacji, aparatu, kalendarza itd.

Po skonfigurowaniu wszystkich ustawień możesz zapisać politykę i zastosować ją na urządzeniach ręcznie lub przypisując ją do określonych grup użytkowników bądź urządzeń. Będą one teraz zabezpieczone i gotowe do pracy w trybie COBO.