



Instrukcja Administratora - Szablony polityk



www.famoc.com

PUBLISHED BY

FAMOC S.A.

Ul. Wajdeloty 12A

80-437 Gdańsk

Copyright© 2008-2022 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. Lista szablonów polityk	6
1.1 Odśwież polityki na urządzeniach	8
1.2 Okienko statusu polityk	9
2. Szablony polityk pełnego zarządzania	10
2.1 Ustawienia podstawowe	10
2.1.1. Ustawienia harmonogramów	12
2.2 Przypisane grupy	14
2.3 Elementy polityk	15
2.4 Opcje bezpieczeństwa	16
2.4.1 Reguły czasowe/lokalizacji/prędkości	16
2.4.2 Polityka czyszczenia danych	18
2.4.3 Polityka sieci	19
2.4.4 Polityka lokalizacji	23
2.4.5 Polityka aktualizacji	24
2.4.6 Polityka sprzętowa	25
2.4.7 Polityka szyfrowania	31
2.4.8 Polityka instalatora	31
2.4.9 Ograniczenia aplikacji	33
2.4.10 Polityka aplikacji	40
2.4.11 Samsung KSP	42
2.5 Zaawansowane	43
3. Szablony polityk BYOD/WPC	48
3.1 Ustawienia podstawowe	48
3.1.1. Ustawienia harmonogramów	50
3.2 Przypisane grupy	51
3.3 Elementy polityk	52
3.4 Opcje bezpieczeństwa	53

3.5 Włączone aplikacje i widgety	61
3.6 Zaawansowane	62
4. Polityki COSU	66
4.1 Ustawienia podstawowe	66
4.1.1. Ustawienia harmonogramów	67
4.2 Przypisane grupy	69
4.3 Elementy polityk	69
4.4 Ustawienia trybu COSU	70
4.5 Opcje bezpieczeństwa	72
4.5.1 Polityka czyszczenia danych	72
4.5.2 Polityka sieci	73
4.5.3 Polityka lokalizacji	75
4.5.4 Polityka aktualizacji	76
4.5.5. Polityka sprzętowa	76
4.5.6 Polityka szyfrowania pamięci	77
4.5.7 Polityka instalatora	78
4.5.8 Ograniczenia aplikacji	78
4.5.9 Polityka aplikacji	79
4.5.10 Samsung KSP	80
4.6 Zaawansowane	81
5. Polityki urządzeń współdzielonych	83
5.1 Ustawienia podstawowe	83
5.1.1 Ustawienia harmonogramów	84
5.2 Przypisane grupy urządzeń	85
5.3 Elementy polityki	85
5.4 Opcje bezpieczeństwa na urządzeniu	86
5.4.1 Polityka aktualizacji	86
5.4.2 Polityka sprzętowa	87
5.5 Ustawienia profilu użytkownika	87
5.5.1 Ograniczenia profilu do pracy	87

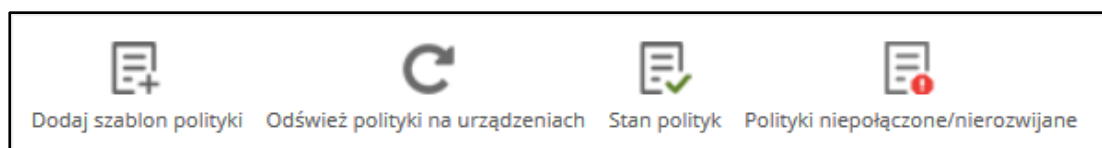
5.5.2 Włączone aplikacje	88
5.6 Zaawansowane	88
6. Status polityk na stronie szczegółów urządzenia	89

1. Lista szablonów polityk

Od wersji FAMOC 5.8 szablony polityk będą rozdzielone dla urządzeń w pełni zarządzanych i BYOD. W zależności od wyboru podczas procesu rejestracji zastosowany zostanie odpowiedni typ polityki.

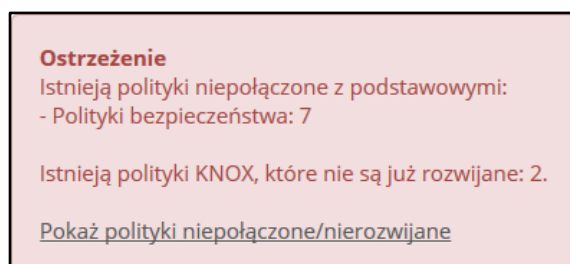
Aby rozpocząć konfigurację polityk przejdź do zakładki **ZARZĄDZANIE** → **Ustawienia** → **Polityki**. Możliwe akcje główne (przyciski na górze listy):

1. **Dodaj szablon polityk** - umożliwia administratorowi utworzenie nowego szablonu zasad
2. **Odśwież polityki na urządzeniach** - umożliwia administratorowi zastosowanie polityk na wielu urządzeniach.
3. **Stan polityk** - zawiera przegląd urządzeń przypisanych do poszczególnych polityk, zgodnych urządzeń, urządzeń z nieaktualną polityką i urządzeń, na których zasady nie zostały jeszcze zaimplementowane.
4. **Polityki niepołączone/nierozwijane** - jeśli używano poprzednich wersji FAMOC-a, znajdziesz w tym miejscu wszystkie poprzednio używane szablony polityk, które nie zostały połączone lub są już nierozwijane.



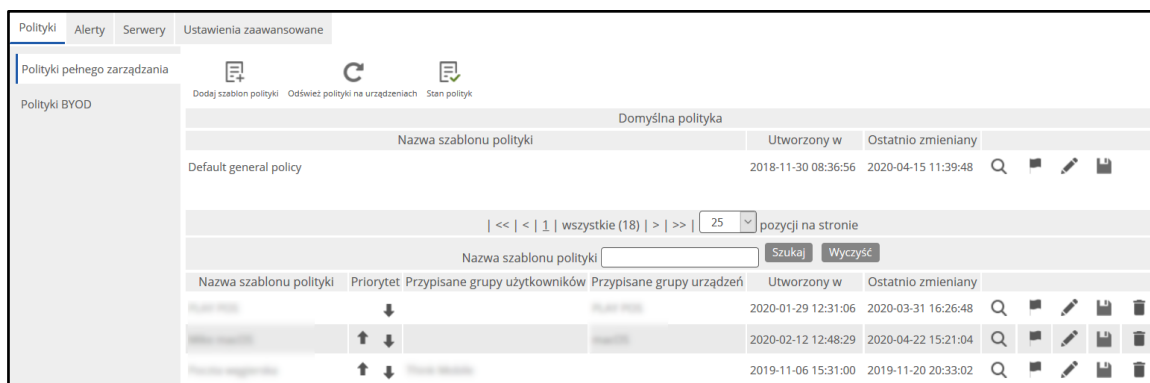
Rysunek 1 Przyciski akcji głównych

Jeśli istnieją wcześniej używane polityki, które nie zostały połączone, wyświetli się ostrzeżenie.



Rysunek 2 Ostrzeżenie o niepołączonych/nierozwijanych politykach

Proces łączenia polityk opisano w szczegółach [tutaj](#).



Rysunek 3 Szablony polityk

UWAGA: Domyślna polityka znajduje się teraz na górze listy i nie można przypisać do niej grup. Polityka ta jest stosowana do urządzeń, które nie są przypisane do żadnej innej polityki. Dla obu grup urządzeń (pełne zarządzanie oraz BYOD) istnieją osobne polityki domyślne.

Poszczególne kolumny zawarte na liście szablonów polityk:

1. **Nazwa szablonu polityki** – nazwa szablonu (kliknięcie nazwy otwiera stronę edycji polityki)
2. **Priorytet** – kolejność wyboru szablonu polityki dla urządzeń (jeśli użytkownik nie jest przypisany do żadnej z grup powiązanych z istniejącymi szablonami - ostatni szablon zostanie zastosowany dla urządzeń użytkownika, jeśli użytkownik jest przypisany do jednej z grup powiązanych z istniejącymi szablonami - na urządzeniach użytkownika zostanie zastosowany szablon polityki o najwyższym priorytecie). Kliknięcie na zielone strzałki zmienia kolejność.
3. **Przypisane grupy użytkowników** - grupy użytkowników przypisane do szablonu
4. **Przypisane grupy urządzeń** – grupy urządzeń przypisane do szablonu
5. **Utworzony w** – data utworzenia szablonu polityki
6. **Kolumna akcji** – opisana szczegółowo w tabeli poniżej:

Działanie	Ikona	Opis
Podgląd		Wyświetla szczegóły szablonu (bez możliwości edycji)
Pokaż status polityki		Otwiera okienko z przeglądem urządzeń przypisanych do zasad, zgodnych urządzeń, urządzeń z nieaktualną polityką i urządzeń, na których zasady nie zostały jeszcze zaimplementowane
Edytuj		Otwiera formularz edycji.
Zapisz jako		Zapisz istniejącą politykę jako nową.
Usuń		Dodaje możliwość usunięcia szablonu polityki (tylko wtedy, gdy szablon nie jest obecnie stosowany na żadnym z urządzeń). Jeśli szablon jest obecnie stosowany - zostanie wyświetlony komunikat alertu

		("Szablon polityk jest już stosowany na urządzeniach i nie można go usunąć").
--	--	---

1.1 Odśwież polityki na urządzeniach

Kliknięcie przycisku **Odśwież zasady na urządzeniach** przekierowuje do strony operacji wysyłania. Lista urządzeń jest automatycznie uzupełniana o wszystkie urządzenia, które wymagają przypisania polityk (urządzenia z nieaktualnymi zasadami i dla których zasady nie są przypisane, ale mają zainstalowane agenty).

Operacja:

Odśwież politykę

Lista urządzeń (58) Wybierz urządzenia

Nazwa urządzenia	ID urządzenia	Status
...	...	X Brak karty SIM w telefonie
...	...	X
...	...	X
...	...	X
...	...	X
...	...	X
...	...	X Brak karty SIM w telefonie

Ustawienia dodatkowe:

☒ Wykonaj operację teraz

☐ Wybranego dnia: 2019-09-30 o godzinie 11:07 + losowo 0

☐ Wykonaj operację później (operacja zostanie wykonana gdy urządzenie połączy się z serwerem, okres zależy od ustawień Agenta Bazowego)

☐ Wykonaj operację później, zaczynając: 2019-09-30 o godzinie 11:07 + losowo 0

Powrót Wyślij

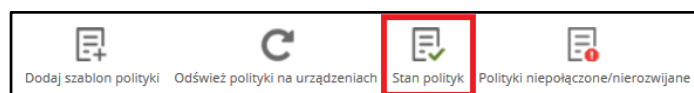
Rysunek 4 Strona operacji odświeżania polityki

Możesz wybrać czy chcesz przeprowadzić operację natychmiast lub zaplanować ją na później. Aby potwierdzić swój wybór kliknij **Wyślij**.

1.2 Okienko statusu polityk

Kliknięcie przycisku **Stan polityk** otwiera okno ze wszystkimi stanami polityk. Wyskakujące okno zawiera przegląd urządzeń przypisanych do poszczególnych polityk, zgodnych urządzeń, urządzeń z nieaktualną polityką i urządzeń, na których polityki nie zostały jeszcze zaimplementowane.

Kliknięcie ikony podglądu powoduje wyświetlenie listy urządzeń.



Status polityki

Dane szablonu polityki

Nazwa szablonu polityki:

Default general policy

Rodzaj szablonu polityki:

Polityka

Data ostatniej modyfikacji:

2019-09-11 13:35:37

Stan polityki

Urządzenia przypisane do polityki:

7

Urządzenia zgodne z polityką:

1

Urządzenia niezgodne z aktualną polityką:

0

Urządzenia, na których polityka nie powiodła się:

0

Urządzenia, na których polityka została ręcznie usunięta:

0

Urządzenia, na których polityka nie jest jeszcze wprowadzona:

6

Odśwież politykę

Zamknij

Rysunek 5 Okno statusu polityk

Status polityki - Lista urządzeń - Wszystkie

| << | < | 1 | wszystkie (7) | > | >> |

Użytkownik	IMEI	Device UID	Numer seryjny	Model	Data ostatniego statusu	Status	
...	...	...	...	Huawei Mate 20 Lite		*	
...	...	...	...	Nokia 5		*	
...	...	...	...	Samsung SM-J530G Galaxy J5 2017		*	
...	...	...	...	Samsung SM-J415FN Galaxy J4 Plus		*	
...	...	...	...	Oppo A5		*	
...	...	...	...	Nokia 3		*	
...	...	...	...	Apple iPad Air	2019-09-30 09:35:53	✓	

| << | < | 1 | wszystkie (7) | > | >> |

Odśwież politykę

Zamknij

Rysunek 6 Status polityk - lista urządzeń

Lista urządzeń zawiera następujące parametry:

1. **Użytkownik** - użytkownik urządzenia
2. **IMEI, Device UID, Numer seryjny** – identyfikator urządzenia
3. **Model** – model urządzenia

4. **Data ostatniego statusu** – data, kiedy polityki zostały pomyślnie zastosowane
5. **Ikona bieżącego statusu**
6. **Kolumna akcji** - z możliwością odświeżenia polityki na wybranym urządzeniu (przez kliknięcie ).

Istnieje możliwość odświeżenia polityki na wszystkich urządzeniach z nieaktualną lub nieprzypisaną polityką (Przycisk **Odśwież politykę** na dole okna).

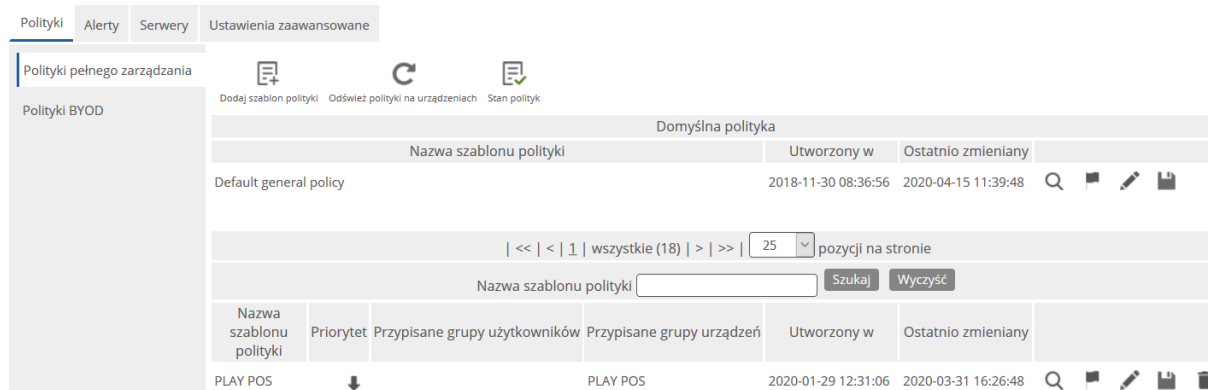
Status polityki jest opisany w następujący sposób:

- Jeśli urządzenie nie ma przypisanego szablonu polityki - kolor tekstu jest szary, a ikona stanu to .
- Jeśli szablon polityki nie działa poprawnie na urządzeniu - jego kolor jest czerwony, a ikona stanu to .
- Jeśli urządzenie ma nieaktualny szablon polityk (szablon zasad został zmieniony po zastosowaniu zasad na urządzeniu) - kolor tekstu jest pomarańczowy, a ikona stanu to .
- Jeśli urządzenie jest zgodne z polityką - kolor tekstu jest zielony, a ikona stanu to .

2. Szablony polityk pełnego zarządzania

Aby dodać nową politykę, kliknij przycisk **Dodaj szablon polityki**.

Aby edytować istniejącą politykę, kliknij jej nazwę lub przycisk **Edytuj**.



Rysunek 7 Główny widok polityk

2.1 Ustawienia podstawowe

Aby dodać ogólny szablon polityk, podaj nazwę i ustaw priorytet.

Atrybut	Opis
---------	------

Ustawienia podstawowe	
Nazwa szablonu	Wprowadź nazwę polityki (maks. 100 znaków)
Ustaw priorytet	Określ pozycję na liście szablonów
Przeinstaluj Base Agenta automatycznie	Po pojawieniu się w systemie nowej wersji programu Base Agent zostanie ona automatycznie ponownie zainstalowana na urządzeniach (polityka zostanie ustawiona jako nieaktualna). Wartość domyślna: niezaznaczone.
Odinstaluj niezgodne elementy polityki automatycznie	Jeśli ta opcja jest zaznaczona, niepasujące elementy z bieżącej polityki zostaną odinstalowane, jeśli urządzenie zostanie przypisane do innej polityki. Wartość domyślna: niezaznaczone.
Włącz Samsung Premium API	Aby aktywować Samsung Premium API w polityce, należy zaznaczyć tę opcję ¹ . Należy również podać odpowiedni klucz licencyjny. Wartość domyślna: niezaznaczone.
Licencja premium	Licencja Samsung Premium może być dodana/zmieniona /usunięta przy użyciu ikon plus/minus obok pola klucza licencyjnego.
Włącz atestację Samsung	Jeśli ta opcja jest zaznaczona, dodatkowa operacja dla atestacji Samsung KNOX zostanie dodana do kolejki i sprawdzi integralność oprogramowania urządzenia przed utworzeniem kontenera KNOX. Wartość domyślna: niezaznaczone.
Oznacz urządzenie jako wyczyszczone przy wykrytym odinstalowaniu Agenta Bazowego	Jeśli ta opcja jest zaznaczona, urządzenie zostanie oznaczone w konsoli FAMOC jako wyczyszczone w przypadku odinstalowania Agenta Bazowego. Wartość domyślna: niezaznaczone.
Włącz usługi zdalnego pulpitu	Jeśli ta opcja jest zaznaczona, Zdalny dostęp zostanie zainstalowany wraz z polityką. Wartość domyślna: niezaznaczone.
Włącz usługi lokalizacyjne	Jeśli ta opcja jest zaznaczona, Monitor lokalizacji zostanie zainstalowany wraz z polityką. Wartość domyślna: niezaznaczone.
Interwał lokalizacji	Interwał, w którym sprawdzana jest lokalizacja urządzenia. Wartość domyślna: Off

¹ Możesz przeczytać więcej o zaletach oferowanych przez KPE Premium tutaj: [Knox Platform for Enterprise | Advanced mobile security management](#)

Wyłączanie raportowania lokalizacji poza szczytem	Po ustawieniu lokalizacja nie zostanie pobrana z urządzenia poza szczytem. Wartość domyślna: nie zaznaczone
Wyłączanie raportowania lokalizacji po instalacji agenta	Po ustawieniu lokalizacja nie zostanie pobrana zaraz po zainstalowaniu agenta. Wartość domyślna: nie zaznaczone
Wymuszaj włączenie usługi monitorowania aplikacji	Po ustawieniu dodatkowa operacja zawarta w ogólnej polityce o nazwie "Włącz usługi monitorowania aplikacji" zostanie dodana do kolejki i wysłana do urządzenia z prośbą o włączenie przez użytkownika Usługi dostępności FAMOC.
Ignoruj optymalizację zużycia baterii dla Monitora lokalizacji i Monitora użycia	Po ustawieniu, do kolejki zostanie dodana dodatkowa operacja zawarta w polityce ogólnej, o nazwie „Włącz usługę monitorowania aplikacji” i wysłana do urządzenia z prośbą o włączenie usługi dostępności FAMOC.
Raportuj dodatkowe informacje o aplikacjach (rozmiar aplikacji, rozmiar pamięci podręcznej, rozmiar danych)	Po zaznaczeniu tej opcji FAMOC będzie zbierać informacje o pamięci zajmowanej przez aplikację i jej pliki
Raportowane aplikacje	Dostępne opcje: • Raportuj wszystkie aplikacje • Raportuj tylko zarządzane aplikacje

Ustawienia podstawowe

Nazwa szablonu:

Ustaw priorytet:

Przeinstaluj Base Agent automatycznie: ☐

Odinstaluj niezgodne elementy polityki automatycznie: ☐

Włącz Samsung Premium API: ☒

Licencja premium: - - - - - +

Włącz atestację Samsung: ☐

Włącz atestację Safetynet: ☐

Oznacz urządzenie jako wyczyszczone przy wykrytym odinstalowaniu Agentu Bazowego: ☐

Włącz usługi zdalnego pulpitu: ☐

Włącz usługi lokalizacyjne: ☐

Wymuszaj włączenie usługi monitorowania aplikacji: ☐

Ignoruj optymalizację zużycia baterii dla Monitora lokalizacji i Monitora użycia *: ☐

Rysunek 8 Zakładka ustawień podstawowych

2.1.1. Ustawienia harmonogramów

Poniżej znajduje się lista parametrów ustawień harmonogramów polityk.

Atrybut	Opis
---------	------

Ustawienia harmonogramów	
Interwał synchronizacji w szczycie	Interwał połączenia z serwerem Base Agent: 5 min./15 min./30 min./1 g./4 g./12 g./Raz dziennie/Raz w tygodniu/Raz w miesiącu Wartość domyślna: raz dziennie
Dni szczytu	Dni tygodnia, w trakcie których Agent Bazowy raportuje do serwera FAMOC Wartość domyślna: od poniedziałku do piątku
Początek szczytu	O której godzinie w dniach szczytu powinien zacząć raportowanie agent podstawowy Wartość domyślna: 8:00
Koniec szczytu	O której godzinie w dniach szczytu powinien zakończyć raportowanie agent podstawowy Wartość domyślna: 16:00
Interwał sesji Monitora Urządzenia	Ustawia interwał sesji Monitora Urządzenia: Wyłączony/Co godzinę, 4 razy dziennie/Codziennie/Raz w tygodniu/Raz w miesiącu Wartość domyślna: Codziennie
Informowanie o nieaktywności urządzenia	Ostrzeganie o bezczynności agenta bazowego po: 1-5 dniach/tygodniu/miesiącu/3 miesiącach. Jeśli agent bazowy nie połączy się z serwerem w tym okresie, FAMOC wygeneruje alert z trzema możliwymi opcjami reakcji: • Usuń urządzenie z FAMOC • Zainstaluj ponownie program Base Agent • Oznacz urządzenie jako skradzione Wartość domyślna: po tygodniu
Wyczyść urządzenie przy przekroczonej nieaktywności	Jeśli ta opcja jest zaznaczona, a agent bazowy nie zgłasza się do serwera w określonym czasie, oprócz wygenerowanego alertu urządzenie zostanie wyczyszczone.
Oznacz urządzenie jako wyczyszczone przy przekroczonej nieaktywności	W przypadku przekroczenia czasu zgłoszenia się urządzenia do serwera, zostanie ono oznaczone w konsoli FAMOC jako wyczyszczone.

Ustawienia harmonogramów

Interwał synchronizacji w szczycie:

Raz dziennie

Dni szczytu:

☒ Poniedziałek
☒ Wtorek
☒ Środa
☒ Czwartek
☒ Piątek
☐ Sobota
☐ Niedziela

Początek szczytu:

08:00

Koniec szczytu:

16:00

Interwał sesji Monitora urządzenia:

Dzień

Informowanie o nieaktywności urządzenia:

Po tygodniu

Wyczyść urządzenie przy przekroczonej nieaktywności:

☐

Oznaczyć urządzenie jako wyczyszczone przy przekroczonej nieaktywności:

☐

Rysunek 9 Ogólne ustawienia polityk

2.2 Przypisane grupy

Każda polityka przypisana jest do określonych grup użytkowników lub grup urządzeń, dlatego każde urządzenie otrzymuje ustawienia polityk wstępnie zdefiniowane do przypisanej grupy. Urządzenia nienależące do żadnej grupy oraz grupy, które nie są przypisane do żadnej polityki, otrzymują politykę o najniższym priorytecie (polityka znajdująca się na dole listy). Urządzenia przypisane do kilku grup otrzymują politykę o wyższym priorytecie.

W zakładce **Grupy** administrator może przydzielać grupy do polityk. Aby wybrać grupę, kliknij przycisk **Dodaj grupę urządzeń** lub przycisk **Dodaj grupę użytkowników**. Zostanie wyświetlone okno z listą grup.

Grupy użytkowników

Lista przypisanych grup użytkowników

Dodaj grupę użytkowników

Nazwa grupy	Liczba użytkowników	Przypisani użytkownicy	
-------------	---------------------	------------------------	--

Rysunek 10 Zakładka Przypisane grupy

Zaznacz pola wyboru obok odpowiednich grup i kliknij Wybierz. Grupy zostaną teraz przypisane do polityki.

▼

Grupy użytkowników

Lista przypisanych grup użytkowników

Dodaj grupę użytkowników

Nazwa grupy	Liczba użytkowników	Przypisani użytkownicy	
Harvey Group	1	Harvey Specter	×
Harvey BYOD	1	Harvey BYOD	×
Harvey Secure	1	Harvey Secure	×

2.3 Elementy polityk

Oprócz ogólnych ustawień istnieje możliwość dodania konfiguracji i aplikacji do polityki.

Aby dodać konfigurację do polityki, kliknij przycisk **Wybierz konfigurację**. Pojawi się okno z listą konfiguracji.

Konfiguracja może być ustawiona dla:

- Szczytu – konfiguracja zostanie zastosowana w okresie szczytu
- Poza szczytem – konfiguracja zostanie zastosowana poza okresem szczytu
- Zawsze – konfiguracja będzie zawsze stosowana

Za każdym razem, gdy urządzenie łączy się z serwerem, sprawdza, czy zastosowana jest odpowiednia polityka, a jeśli potrzebna jest zmiana (np. zakończył się okres szczytu, a aktualnie stosowana konfiguracja dotyczy tylko tego okresu), stara konfiguracja jest usuwana, a zastosowana jest odpowiednia. Polityki oparte na czasie mogą być stosowane tylko na urządzeniach z systemem iOS.

Aby dodać aplikację, kliknij przycisk **Wybierz aplikację**. Pojawi się okno z listą aplikacji. Wybrane aplikacje zostaną zainstalowane podczas przypisywania polityk do urządzenia. Po zmianie polityk przypisanych do urządzenia zastosowane zostaną nowe polityki i zainstalowana nowa lista aplikacji. Podczas wyboru aplikacji, można określić liczbę powtórzeń instalacji (w przypadku anulowania instalacji przez użytkownika, FAMOC ponowi operację). Możliwe opcje:

- Instalacja obowiązkowa (opcja domyślna) - jeśli instalacja zostanie anulowana, będzie powtarzana co dzień.
- Jedna próba instalacji - jeśli instalacja zostanie anulowana, nie będzie ponawiana.
- Kilka prób instalacji - instalacja będzie ponawiana określoną liczbę razy.

Elementy polityki można ustawić w niestandardowej kolejności instalacji, używając strzałek w dół/w górę w kolumnie **Kolejność**.

Domyślnie każdy element jest instalowany w sekwencji (następny element rozpoczyna się po pomyślnym zainstalowaniu poprzedniego). Można jednak oznaczyć element jako niezależny (kolumna **Niezależny**), co oznacza, że kolejna akcja rozpoczyna się niezależnie od poprzedniej, nie czekając na raport z powodzeniem.

Zaznacz opcję **Ignoruj błąd**, aby wykonać następną akcję, jeśli poprzednia zakończyła się niepowodzeniem.

Elementy polityki					
Nazwa elementu		Akcja	Ignoruj błąd	Niezależny	Kolejność
Require 4 chars lock code on Android	Polityka szczytu:	Zawsze ▾	☐	☐	↓ ×
Tapeta FF 1080p	Polityka szczytu:	Zawsze ▾	☐	☐	↑ ×

Rysunek 11 Elementy polityki

2.4 Opcje bezpieczeństwa

W ramach opcji bezpieczeństwa dostępne są następujące ustawienia:

1. Reguły czasowe/lokalizacji
2. Polityka czyszczenia danych
3. Polityka sieci
4. Polityka lokalizacji
5. Polityka aktualizacji
6. Polityka sprzętowa
7. Polityka szyfrowania pamięci
8. Polityka instalatora
9. Ograniczenia aplikacji
10. Polityka aplikacji

2.4.1 Reguły czasowe/lokalizacji/prędkości

W tej zakładce administrator może dodawać ograniczenia dla Polityk oparte o **Czas**, **Lokalizację (Geofence)** oraz **Prędkość** poruszania się urządzenia. Aby ustawić ograniczenia kliknij **Dodaj regułę**. Wyświetli się okienko **Nowego ograniczenia**.

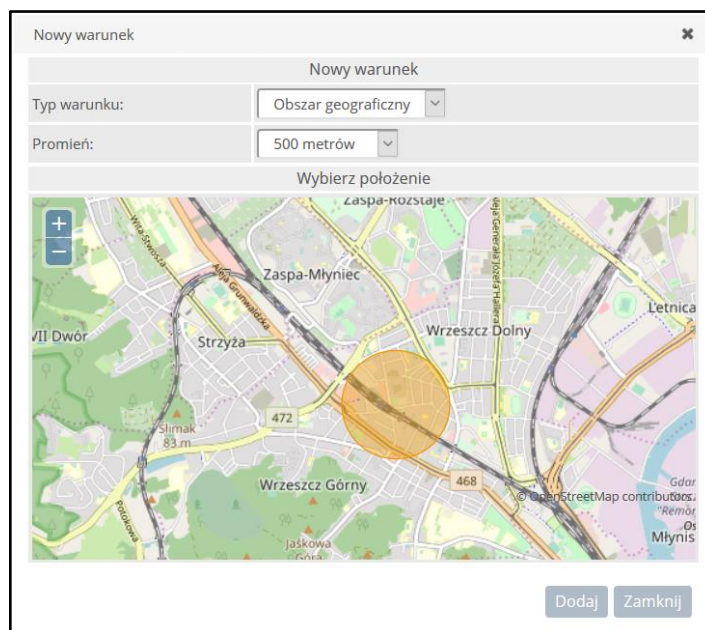
Rysunek 12 Okienko "Nowe ograniczenie"

Następnie administrator dodaje warunek ograniczenia.

Typ warunku: Czasowy - określa, kiedy obowiązuje ograniczenie. Dostępne są dwa okresy: W szczycie i Poza szczytem.

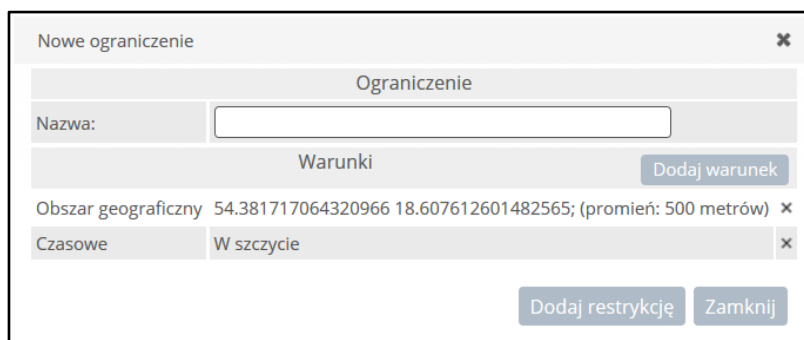
Rysunek 13 Typ warunku: Czasowy

Typ warunku: **Obszar geograficzny**- określ strefę, w której obowiązuje polityka. Wybierz promień z listy (od 500 m do 5000 m) i wybierz punkt na mapie. Podczas dodawania warunku poprzednie zaznaczenia są widoczne na mapie.



Rysunek 14 Typ warunku: Obszar geograficzny: promień 500 m

Przy jednym ograniczeniu można zdefiniować tylko jeden warunek czasowy i geograficzny.



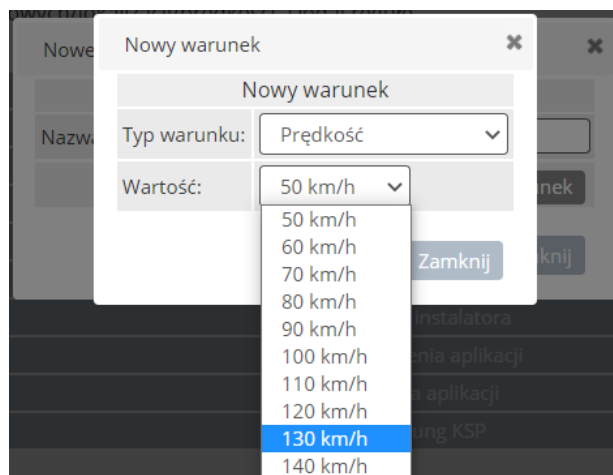
Rysunek 15 Warunki czasowe i geograficzne przy jednym ograniczeniu

Ograniczenie prędkości pozwala na zmianę ustawień polityki w zależności od prędkości ruchu urządzenia. Przykład:

- W polityce ustawiamy jako limit prędkości 140 km/h.
- W momencie przekroczenia danej prędkości następuje zmiana polityki np. wyłączone są aplikacje społecznościowe, aparat itp.
- Możemy również ustawić np. tzw białą listę i określić że w momencie przekroczenia określonego progu na urządzeniu będą dostępne tylko aplikacje takie jak Mapy.
- W momencie, gdy prędkość spadnie poniżej określonego limitu przywrócone zostaną standardowe ustawienia polityki.

Przy pomiarze stosowany jest dziesięcioprocentowy margines błędu.

UWAGA: Jeśli średnia prędkość rośnie / spada, polityka ulega zmianie. Jeśli prędkość lokalizacji nie jest dostępna, a ostatnia prędkość była powyżej zera, będziemy ją zmniejszać o jeden km / h aż do zera co sekundę.



2.4.2 Polityka czyszczenia danych

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka czyszczenia danych**.

Atrybut	Opis
Polityka czyszczenia danych	
Czyszczenie pamięci telefonu po wykryciu zmiany karty SIM	Jeśli ustawione, czyszczenie zostanie wykonane po wykryciu zmiany karty SIM. Dostępność: urządzenia z systemem Android
Reaguj również na brak karty	Jeśli ustawione, czyszczenie zostanie wykonane, gdy karta SIM nie zostanie wykryta. Opcja dostępna po ustawieniu pierwszej opcji (Czyszczenie danych przy zmianie karty SIM). OSTRZEŻENIE! Po zastosowaniu tej konfiguracji użytkownicy nie będą mogli korzystać z trybu samolotowego Androida, ponieważ spowoduje to wymazanie urządzenia. Dostępność: urządzenia z systemem Android
Wyczyść również kartę pamięci	Jeśli ustawione, po wykryciu zmiany karty SIM dodatkowo zostanie wyczyszczona karta pamięci. Opcja dostępna po ustawieniu pierwszej opcji (Czyszczenie danych przy zmianie karty SIM). Dostępność: urządzenia z systemem Android
Czyszczenie danych korporacyjnych po wykryciu jailbreak	Jeśli ustawione, dane korporacyjne (wszystkie zainstalowane przez FAMOC MDM) na urządzeniu zostaną usunięte po wykryciu jailbreak. Dostępność: urządzenia z systemem iOS.

Czyszczenie urządzenia po wykryciu rootowania	Jeśli ustawione, urządzenie zostanie wyczyszczone po wykryciu rootowania. Dostępność: urządzenia z systemem Android.
Pozwalaj na blokadę aktywacji	Jeśli jest włączona, opcja Blokada aktywacji zostanie włączona na urządzeniach z systemem iOS Dostępność: urządzenia iOS w trybie nadzorowanym
Blokada przywracania ustawień fabrycznych	Jeśli włączona, uniemożliwia wykonanie resetu do ustawień fabrycznych. Dostępność: Device Owner, Android Samsung 4.x z Enterprise SDK 2.0, Android LG z Enterprise SDK from 1.0 , Windows Phone 8.1/10
Ochrona przywracania do ustawień fabrycznych (FRP)²	Factory Reset Protection to rozwiązanie, które umożliwia uruchomienie urządzenia po przywróceniu ustawień fabrycznych jedynie kontem Google, którym wcześniej zalogowano się na urządzeniu. Dostępne możliwości konfiguracji tego ustawienia: - wyłączona (opcja nie będzie dostępna) - odblokuj urządzenie aktywnym kontem (urządzenie można odblokować poprzednio używanym kontem) - odblokuj urządzenie za pomocą konta z listy (urządzenie można odblokować kontem z wprowadzonej listy - należy podać id użytkownika) - zdejmij blokadę FRP po wyczyszczeniu urządzenia (wyłącza blokadę po wyczyszczeniu urządzenia) Dostępność: Device Owner

2.4.3 Polityka sieci

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka sieci**.

Atrybut	Opis
Polityka sieci	
Blokada interfejsu Wi-Fi	Jeśli włączona na urządzeniu niemożliwe będzie korzystanie z Wi-Fi. Dostępność: urządzenia z systemem Android i Windows Phone 8.1 / 10

² Lista kont do odblokowania musi zawierać prawidłowe identyfikatory użytkownika Google. Można je uzyskać z Google API, korzystając z linku poniżej:

<https://developers.google.com/people/api/rest/v1/people/get>

Wykonując wywołanie interfejsu API i logując się przy użyciu prawidłowego konta Google, odpowiedź zwraca „id” użytkownika.

Blokada automatycznego łączenia do punktów dostępowych Wi-Fi	Jeśli włączona, urządzenie nie będzie się automatycznie łączyć z punktami dostępowymi Wi-Fi. Dostępność: Windows Phone 8.1 / 10
Blokada raportowania punktów dostępowych Wi-Fi	Jeśli włączona, urządzenie nie będzie raportować punktów dostępowych Wi-Fi. Dostępność: Windows Phone 8.1
Blokada ręcznej konfiguracji Wi-Fi	Jeśli włączona, nie będzie możliwości ręcznej konfiguracji Wi-Fi. Dostępność: Tryb Device Owner, urządzenia iOS w trybie nadzorowanym, Windows Phone 8.1 / 10
Blokada modyfikacji prywatnych punktów dostępowych	Jeśli włączona, nie będzie możliwości ręcznej modyfikacji APN (prywatnych punktów dostępowych). Dostępność: Urządzenia iOS w trybie nadzorowanym
Utrzymuj Wi-Fi włączone w trybie uśpienia	Jeśli ustawione, zapobiega rozłączeniu Wi-Fi w trybie uśpienia. Dostępność: Tryb Device Owner
Zapobiegaj wyłączeniu Wi-Fi	Zapobiega wyłączaniu Wi-Fi w Ustawieniach lub Centrum sterowania. Dostępność: iOS 13.0
Blokada interfejsu Bluetooth	Jeśli włączona, na urządzeniu nie może być używana komunikacja Bluetooth. Dostępność: Android, Windows Phone 8.1 / 10, iOS 11.3 i nowsze w trybie nadzorowanym Możliwe opcje dla systemu Android Samsung z pakietem Enterprise SDK od wersji 2.0: - Włącz profil zaawansowanej dystrybucji audio (A2DP) - Włącz profil zdalnego sterowania audio/wideo (AVRCP) - gdy ten profil jest włączony z (A2DP) użytkownik będzie mógł korzystać z połączenia Media Audio, dodatkowo użytkownik będzie mógł używać przycisków na urządzeniu Bluetooth (Play/Stop/Następny utwór) - Włącz profil głośnomówiący (HFP) - ten profil działa tylko z profilem HSP - Włącz profil bezprzewodowego zestawu słuchawkowego (HSP) - gdy ten profil jest włączony z (HFP) użytkownik będzie mógł korzystać z połączenia Call Audio, dodatkowo użytkownik będzie mógł używać przycisków na urządzeniu Bluetooth (Odbierz lub przerwij połączenie) - Włącz profil dostępu do książki telefonicznej (PBAP) - po włączeniu tego profilu urządzenie bluetooth będzie

	miało dostęp do kontaktów zapisanych na telefonie lub tablecie - Włącz profil wirtualnego portu szeregowego (SPP) - ten profil musi zostać wybrany, aby zapewnić prawidłowe połączenie bezprzewodowe pomiędzy urządzeniami - Włącz udostępnianie plików przez Bluetooth
Blokada danych pakietowych	Możliwe opcje: • Nie blokuj • Włącz i zablokuj możliwość wyłączenia • Wyłącz i zablokuj możliwość włączenia Dostępność: Android Wartość domyślna: Nie blokuj.
Blokada danych pakietowych w roamingu	Możliwe opcje: • Nie blokuj • Wyłącz i zablokuj możliwość włączenia Dostępność: Android, Tryb Device Owner i urządzenia Windows Phone 8.1 / 10 Wartość domyślna: Nie blokuj.
Wyłącz możliwość modyfikacji planu komórkowego	Blokuje możliwość zmiany obowiązującego planu taryfowego
Blokada udostępniania internetu przez WiFi	Jeśli włączona, udostępniania internetu przez WiFi zostanie wyłączone. Dostępność: Android Samsung z Enterprise SDK od 2.0 i Tryb Device Owner
Blokada udostępniania internetu przez USB	Jeśli włączona, udostępnianie internetu przez USB jest wyłączone. Dostępność: Android Samsung z Enterprise SDK od 3.0, Tryb Device Owner oraz Windows Phone 8.1 / 10
Blokada VPN przez sieć komórkową	Jeśli włączona, VPN nie może być używany podczas korzystania z danych komórkowych. Dostępność: Windows Phone 8.1 / 10
Blokada raportowania użycia urządzenia do Microsoftu	Jeśli włączona, raport użycia wysyłany do firmy Microsoft zostanie wyłączony. Dostępność: Windows Phone 8.1/10
Blokada VPN przez sieć komórkową w roamingu	Jeśli włączona, VPN nie może być używany podczas korzystania z danych komórkowych w roamingu. Dostępność: Windows Phone 8.1/10

Nie zezwalaj na tworzenie konfiguracji VPN	Jeśli włączona, użytkownik nie będzie mógł zmieniać ustawień VPN. Dostępność: iOS 11.0
Blokada przychodzących wiadomości MMS	Jeśli włączona przychodzące wiadomości MMS nie będą dostarczane. Dostępność: Android Samsung z Enterprise SDK from 3.0
Wyłącz możliwość resetowania ustawień sieci	Blokuje możliwość korzystania z opcji "Resetuj ustawienia sieciowe". Dostępność: tryb Device Owner
Wyłącz ustawienia VPN	Blokuje możliwość zmiany ustawień przez użytkownika Dostępność: Android, Device Owner
Wyłącz możliwość modyfikacji ustawień eSIM	Jeśli włączono, użytkownik nie będzie mógł zmienić ustawień karty eSIM. Dostępność: iOS 12.1
Blokuj ustawienia prywatnych DNS	Jeśli jest ustawiony, użytkownik nie może ustawić prywatnego DNS ani wyłączyć DNS przez TLS na urządzeniu. Dostępność: Urządzenia w trybie Device Owner z systemem Android 10.0+
Blokada rozmów wychodzących	Blokuje możliwość wykonywania połączeń wychodzących Dostępność: tryb Device Owner
Zablokuj przychodzące rozmowy	Umożliwia blokowanie połączeń przychodzących. Dostępne opcje: • Nie blokuj • Wszystkie • Wg wzoru (Wzór blokowanych numerów może zawierać np. numery rozpoczynające się od 0700) Dostępność: Samsung SDK
Zablokuj przychodzące wiadomości SMS	Umożliwia blokowanie przychodzących wiadomości tekstowych. Dostępne opcje: • Nie blokuj • Wszystkie • Wg wzoru (Wzór blokowanych numerów może zawierać np. numery rozpoczynające się od 0700) Dostępność: Samsung SDK
Blokada edycji zarządzanych sieci	Opcja zapobiega edycji ustawień sieci WiFi zarządzanych przez FAMOC. Dostępność: Android

Monitoruj listę zarządzanych konfiguracji Wi-Fi	Monitoruje stan zarządzanych sieci i wyzwala alert w przypadku ich usunięcia (zapomnienia na urządzeniu).
Blokuj pobieranie w tle podczas roamingu	Wyłącza pobieranie w tle gdy urządzenie jest w roamingu Dostępność: iOS
Blokuj wybieranie głosowe, jeśli urządzenie jest zablokowane hasłem	Dostępność: iOS
Blokuj modyfikację danych komórkowych dla aplikacji	Dostępność: iOS supervised
Blokuj parowanie hostów	Dostępność: iOS supervised
Blokuj konfigurację Bluetooth	Dostępność: Samsung SDK, Device Owner
Blokada konfiguracji sieci mobilnych	Dostępność: Device Owner (Android 8.0 +)
Blokada konfiguracji transmisji komórkowej	Dostępność: Device Owner (Android 8.0 +)
Wyłącz wiadomości SMS	Dostępność: Device Owner (Android 8.0 +)

2.4.4 Polityka lokalizacji

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka lokalizacji**.

Atrybut	Opis
Polityka lokalizacji	
Blokada GPS	Possible options: • Nie blokuj • Włącz GPS • Włącz GPS i zablokuj możliwość wyłączenia • Wyłącz GPS • Wyłącz GPS i zablokuj możliwość włączenia Dostępność: Android Samsung z Enterprise SDK 3.0 Wartość domyślna: Nie blokuj

Aktywacja trybu Tylko GPS	Jeśli jest ustawiony, użytkownik nie może włączyć trybu oszczędzania energii i wysokiej dokładności, tylko GPS jest włączony i nie można go wyłączyć.
Blokada usług lokalizacji	Pozwala przyznać agentowi FAMOC dostęp do lokalizacji i blokuje możliwość cofnięcia tych uprawnień. Możliwe opcje: • Nie blokuj • Włącz lokację • Włącz lokalizację i zablokuj możliwość wyłączenia • Wyłącz lokalizację • Wyłącz lokalizację i zablokuj możliwość włączenia Dostępność: Windows Phone 8.1 / 10
Blokada lokalizacji na urządzenia Android	Pozwala przyznać agentowi FAMOC dostęp do lokalizacji i blokuje możliwość cofnięcia tych uprawnień. Możliwe opcje: • Nie blokuj • Włącz lokację • Włącz lokalizację i zablokuj możliwość wyłączenia • Wyłącz lokalizację • Wyłącz lokalizację i zablokuj możliwość włączenia Dostępność: Android 8.0+

2.4.5 Polityka aktualizacji

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka aktualizacji**.

Atrybut	Opis
Polityka aktualizacji	
Opóźnij widoczność aktualizacji systemu	Jeśli jest włączona, na urządzeniu nie pojawią się żadne informacje o aktualizacjach. Domyślne opóźnienie wynosi 30 dni, chyba że w polu „Opóźnij aktualizację systemu” wybrano inny okres. Dostępność: iOS supervised od 11.3, macOS od 10.13, tvOS od 12.2
Opóźnij widoczność niesystemowych aktualizacji oprogramowania	Jeśli jest włączona, na urządzeniu nie pojawią się żadne informacje o aktualizacjach niezwiązanych z systemem operacyjnym. Domyślne opóźnienie wynosi 30 dni, chyba że w polu „Opóźnij aktualizację systemu” wybrano inny okres. Dostępność: iOS supervised od 11.3, macOS od 10.13, tvOS od 12.2

Opóźnij aktualizację systemu o	Czas przełożenia aktualizacji systemu (1-90 dni). Dostępność: iOS supervised od 11.3, macOS od 10.13, tvOS od 12.2
Opóźnij mniejszą aktualizację oprogramowania o	Umożliwia opóźnienie pośrednich aktualizacji o określony czas od wydania tych uaktualnień
Opóźnij aktualizację oprogramowania innego niż system operacyjny o	Umożliwia opóźnienie aktualizacji nie-systemowych o określony czas od wydania tych uaktualnień
Wymuś opóźnienie wykonania głównej aktualizacji oprogramowania	Umożliwia opóźnienie głównych aktualizacji o określony czas od wydania tych uaktualnień
Opóźnij główną aktualizację oprogramowania o	Okres, w którym aktualizacja zostanie przełożona. Zakres: 1-90 dni.
Kontroluj wersję systemu (Samsung E-FOTA)	Jeśli włączona, umożliwia obsługę E-FOTA. Dostępność: Android Samsung 7.x z Knox 2.7.1+
Polityka aktualizacji OTA	Możliwość zdefiniowania polityki aktualizacji OTA. Dostępne opcje to: • Brak polityki • Automatyczna • Według harmonogramu • Wstrzymana Dostępność: Device Owner (blokuje aktualizację systemu na 30 dni), Android Samsung z Enterprise SDK 3.0
Aktualizacje OTA dla urządzeń Zebra	Możliwość włączenia aktualizacji OTA dla urządzeń Zebra. Dostępność: urządzenia Zebra z systemem Android 7 lub nowszym i wersją MX 9.2 lub nowszą.
Wyłącz automatyczną aktualizację oprogramowania	Po wybraniu tej opcji aktualizacja oprogramowania sprzętowego urządzenia z trybu pobierania jest wyłączona Dostępność: Samsung SDK z licencją premium
Wyłącz automatyczne sprawdzanie aktualizacji	Jeśli zaznaczone, urządzenie nie będzie automatycznie sprawdzać czy pojawiła się nowa aktualizacja. Dostępność: Samsung SDK z licencją premium

2.4.6 Polityka sprzętowa

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka sprzętowa**.

Atrybut	Opis
Polityki sprzętowe	
Blokada aparatu	Jeśli włączona, wyłącza możliwość korzystania z aparatu. Dostępność: tryb Device Owner, Android 4.x, Android Samsung 2.3 – 4.x oraz Windows Phone 8.1/10, iOS
Wyłącz możliwość usunięcia zarządzania	Jeśli włączona, uniemożliwia ręczną dezaktywację administratora urządzenia FAMOC. Dostępność: Android Samsung z Enterprise SDK od 2.0, Android Sony z Enterprise SDK od 6.0, Android LG z Enterprise SDK od 1.0 oraz Windows 10 Mobile
Wyłącz ręczne usuwanie profilu służbowego Android	Jeśli włączona, użytkownik nie będzie miał możliwość usunięcia profilu służbowego. Dostępność: Device Owner, Android 8.0
Blokada trybu odtwarzacza multimediiów przez USB	Jeśli włączona, a urządzenie jest podłączone do komputera przez USB, nie można użyć do w trybie odtwarzacza multimediiów. Dostępność: Android Samsung 4.x z Enterprise SDK 3.0, Android Sony z Enterprise SDK od 5.0
Zezwalaj na uruchamianie urządzeń w trybie odzyskiwania przez niesparowane urządzenie	Jeśli zaznaczone, umożliwia uruchamianie urządzeń do odzyskiwania przez niesparowane urządzenie. Wymaga urządzenia nadzorowanego
Blokada opcji programisty	Uniemożliwia włączenie trybu programowania. Dostępność: tryb Device Owner, Android Samsung z Enterprise SDK 5.0
Blokada menadżera zadań	Jeśli włączona, uniemożliwia korzystanie z menedżera zadań. Dostępność: Android Samsung z Enterprise SDK 3.0
Blokada NFC	Uniemożliwia korzystanie z NFC. Dostępność: Windows Phone 8.1/10, Android Samsung z Enterprise SDK od 2.0, iOS 14.2
Nie zezwalaj na przesyłanie danych za pomocą NFC	Jeśli ustawiona, użytkownik nie może używać NFC do przesyłania danych z aplikacji. Dostępność: tryb Device Owner
Blokada kart pamięci	Uniemożliwia korzystanie z gniazda kart pamięci. Dostępność: Device Owner, Android Samsung with Enterprise SDK from 2.0, Windows Phone 8.1/10
Blokada możliwości kopiowania i wklejania	Uniemożliwia korzystanie z funkcji kopiuj/wklej. Dostępność: Windows Phone 8.1/10

Blokada przechwytywania obrazu	Jeśli włączona, uniemożliwia wykonywanie zrzutów ekranu Dostępność: Device Owner, Windows Phone 8.1/10, Android Samsung z Enterprise SDK od 2.0 oraz urządzenia z iOS
Wyłącz zdalną obserwację ekranu przez aplikację Classroom	Blokuje możliwość podglądania ekranu w aplikacji Classroom Dostępność: iOS 12.0 lub nowszy, macOS 10.14.4
Blokuj automatyczną korektę	Nie będą widoczne sugestie korekty pisowni Dostępność: iOS supervised
Wyłącz Siri możliwość wysyłania zapytań do treści generowanych przez użytkowników	Siri nie będzie wysyłać zapytań do treści generowanych przez użytkowników np. Wikipedia Dostępność: iOS supervised
Blokada trybu przeglądania plików USB	Jeśli włączona, nie będzie możliwości przeglądania plików przez połączenie USB. Dostępność: Device Owner, Windows Phone 8.1/10
Blokada wielu okien	Jeśli włączona, tryb wielu okien nie będzie dostępny na urządzeniu Dostępność: Android Samsung with Enterprise SDK from 4.0
Blokada trybu awaryjnego	Jeśli opcja zostanie ustawiona, na urządzeniu nie będzie dostępny tryb awaryjny. Dostępność: Device Owner, Android Samsung z Enterprise SDK od 4.0
Blokada trybu samolotowego	Jeśli opcja zostanie ustawiona, na urządzeniu nie będzie dostępny tryb samolotowy. Dostępność: Android Samsung z Enterprise SDK od 5.0
Udostępnij akcesoria USB, gdy urządzenie jest zablokowane	Jeśli włączona, urządzenie iOS będzie mogło zawsze mieć dostęp do akcesoriów USB. Dostępność: iOS supervised 11.4.1
Wyłącz monit o skonfigurowanie nowych urządzeń w pobliżu	Jeśli włączona, na urządzeniu nie będzie pojawiać się monit o skonfigurowaniu urządzeń w pobliżu. Dostępność: iOS supervised 11.0
Wyłącz AirPrint	Możliwość wyłączenia usługi AirPrint (drukowanie za pośrednictwem sieci Wi-Fi). Dostępność: iOS supervised 11.0
Wyłącz zapis danych uwierzytelniających AirPrint na iCloud	Jeśli włączona, dane logowania AirPrint nie będą zapisywane w iCloud. Dostępność: iOS supervised 11.0

Wymagaj zaufanych certyfikatów do komunikacji drukowania TLS	Jeśli włączona, wymusza na urządzeniu używanie zaufanych certyfikatów do komunikacji drukowania TLS. Dostępność: iOS supervised 11.0
Wyłącz wykrywanie drukarek AirPrint przy użyciu iBeacon	Jeśli włączona, funkcja iBeacon nie będzie wykrywać i łączyć się z dostępnymi drukarkami. Dostępność: iOS supervised 11.0
Wyłącz przychodzące żądania AirPlay	Jeśli włączona, urządzenie będzie odrzucać przychodzące żądania strumieniowania AirPlay. Dostępność: tvOS
Nie pozwalaj na automatyczne odblokowanie macOS	Jeśli włączona, nie będzie możliwe odblokowanie urządzenia za pomocą Apple Watch. Dostępność: macOS 10.12
Nie pozwalaj na korzystanie z pulpitu i usług dokumentów w chmurze	Jeśli włączona, usługa pulpitu i dokumentów w chmurze będzie niedostępna. Dostępność: macOS 10.12.4
Uniemożliwiaj odblokowanie urządzenia przez Touch ID	Jeśli włączona, nie będzie możliwe odblokowanie urządzenia przy pomocy odcisku palca. Dostępność: iOS, iOS supervised, macOS 10.12
Blokuj modyfikację ustawień biometrii	Jeśli włączona, niemożliwa będzie zmiana ustawień biometrii.
Wymuszony limit czasu biometrii	Czas, po którym użytkownicy muszą wprowadzić swoje hasło zamiast TouchID.
Nie zezwalaj na buforowanie zawartości	Możliwość wyłączenia usługi Content Caching (buforowania zawartości). Dostępność: macOS 10.13 UWAGA: Ta opcja jest przestarzała
Wyłącz wyszukiwanie definicji	Jeśli zaznaczona, wbudowana opcja słownika będzie wyłączona. Dostępność: iOS supervised, macOS 10.11
Wyłącz skróty klawiaturowe	Blokuje możliwość używania skrótów klawiszowych Dostępność: iOS
Wyłącz klawiaturę QuickPath	Jeśli ustawiony, klawiatura QuickPath będzie wyłączona. Dostępność: iOS 13.0
Wyłącz sprawdzanie pisowni klawiatury	Słowa potencjalnie wpisane nieprawidłowo na urządzeniach użytkowników nie będą podkreślane na czerwono Dostępność: iOS

Zapobiegaj uśpieniu urządzenia	Jeśli ustawione, urządzenie nie przejdzie w tryb uśpienia po okresie bezczynności. Dostępność: tvOS 13.0
Zablokuj konfigurację poświadczeń przez użytkowników w zarządzanym magazynie kluczy	Jeśli ustawione, użytkownik nie będzie miał dostępu do niektórych opcji przechowywania poświadczeń, takich jak: Wyświetl certyfikaty użytkownika, Zainstaluj certyfikaty z pamięci urządzenia, Usuń certyfikaty Dostępność: Device Owner
Wyłącz Siri	Możliwość wyłączenia asystenta Siri Dostępność: iOS
Wyłącz Siri kiedy urządzenie jest zablokowane	Zapobiega uruchamianiu Siri na zablokowanym urządzeniu Dostępność: iOS
Wyłącz połączenia z serwerami Siri na potrzeby dyktowania	Jeśli ta opcja jest ustawiona, połączenia z serwerami Siri na potrzeby dyktowania będą wyłączone Dostępność: iOS 14.5
Wyłącz połączenia z serwerami Siri na potrzeby tłumaczenia	Jeśli ustawione, połączenia z serwerami Siri na potrzeby tłumaczenia będą wyłączone Dostępność: iOS 15.0
Blokuj transmisję zdjęć	Jeśli włączona, blokuje transmisję zdjęć w usłudze iCloud Dostępność: iOS
Wyłącz centrum sterowania na zablokowanym ekranie	Jeśli ustawione, Centrum sterowania nie pojawi się na ekranie blokady Dostępność: iOS
Wyłącz automatyczne przysyłanie raportów diagnostycznych do Apple	Jeśli jest ustawiona, raport diagnostyczny nie będzie automatycznie przysyłany do Apple Dostępność: iOS
Blokuj możliwość tworzenia niezauważalnych połączeń TLS	Jeśli jest ustawiona, zapobiega niezauważalnym certyfikatom TLS (Transport Layer Security) na urządzeniach Dostępność: iOS
Blokuj uaktualnienie bazy danych certyfikatów zaufanych	Jeśli jest ustawiona, zapobiega automatycznym aktualizacjom certyfikatów. Dostępność: iOS
Nie pozwalaj na kopie zapasowe książek firmowych	Jeśli ustawione, kopia zapasowa książek Enterprise będzie wyłączona Dostępność: iOS 8.0

Nie pozwalaj na synchronizację metadanych Enterprise Book	Jeśli ta opcja jest ustawiona, synchronizacja metadanych Enterprise Book zostanie wyłączona Dostępność: iOS 8.0
Wyłącz modyfikację ustawień powiadomień	Jeśli włączona, blokuje możliwość zmiany ustawień powiadomień Dostępność: iOS supervised
Wyłącz podgląd historii powiadomień na zablokowanym ekranie	Jeśli ta opcja jest ustawiona, połączenia z serwerami Siri na potrzeby dyktowania będą wyłączone Dostępność: iOS 7.0
Wyłącz podgląd dzisiejszych powiadomień na zablokowanym ekranie	Jeśli ta opcja jest ustawiona, widok historii powiadomień na ekranie blokady będzie wyłączony Dostępność: iOS 7.0
Wyłącz użycie iCloud przez zarządzane aplikacje	Jeśli ta opcja jest ustawiona, zarządzane aplikacje nie będą mogły korzystać z iCloud Dostępność: iOS 8.0
Wymuś użycie hasła do parowania na urządzeniach otrzymujących zadania z tego urządzenia	Jeśli ta opcja jest ustawiona, hasło parowania będzie wymagane, gdy urządzenie odbierze żądania AirPlay z tego urządzenia Dostępność: iOS
Wymuszenie szyfrowania kopii zapasowej	Wymusza szyfrowanie kopii zapasowej Dostępność: iOS
Wyłącz parowanie zegarków	Po zaznaczeniu rozłączy z aktualnie używanym zegarkiem i wyczyści jego ustawienia Dostępność: iOS supervised
Wymuś rozpoznawanie nadgarstka na Apple Watch	Jeśli zaznaczone, wymusza na sparowanym zegarku Apple Watch korzystanie z funkcji wykrywania nadgarstka Dostępność: iOS
Wyłącz modyfikację hasła	Uniemożliwia zmianę hasła Dostępność: iOS supervised, macOS 10.13+
Blokuj możliwość modyfikacji nazwy urządzenia	Uniemożliwia zmianę nazwy urządzenia Dostępność: iOS supervised, tvOS
Wyłącz dyktowanie	Uniemożliwia użytkownikom korzystanie na swoim urządzeniu z funkcji dyktowania. Dostępność: iOS supervised, macOS

Blokuj modyfikację przesyłania danych diagnostycznych	Jeśli ustawione, zmienianie ustawień dotyczących danych diagnostycznych nie jest dozwolone. Dostępność: iOS supervised
Wyłącz Czas przed ekranem	Blokuje funkcję Czas przed ekranem Dostępność: iOS supervised
Blokuj modyfikację tapety ekranu	Uniemożliwia zmianę tapety Dostępność: iOS supervised, macOS 10.13+
Wymuś filtr wulgaryzmów asystenta	Filtr przekleństw Siri będzie stale włączony Dostępność: iOS supervised, macOS

2.4.7 Polityka szyfrowania

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka szyfrowania**.

Atrybut	Opis
Polityki szyfrowania	
Szyfrowanie pamięci wewnętrznej	Jeśli opcja zostanie ustawiona, wymagane będzie szyfrowanie. Dostępność: Android 4.x oraz Android Samsung z Enterprise SDK 2.0/3.0, iOS oraz Windows Phone 8.1/10
Wyłącz tryb bezpiecznego uruchamiania	Jeśli opcja zostanie ustawiona, bezpieczne uruchamianie urządzenia będzie wyłączone. Dostępność: Urządzenia Android devices z zainstalowanym FAMOC Add-On
Aktywacja trybu Common Criteria	Jeśli opcja zostanie ustawiona, urządzenie zostanie sprawdzone pod kątem zgodności z wymaganiami MDFPP (Mobile Device Fundamentals Protection Profile) ³ Dostępność: Samsung SDK, Device Owner (wymagane KNOX Premium API)

2.4.8 Polityka instalatora

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka instalatora**.

Atrybut	Opis
Polityki instalacji	

³ Dodatkowe informacje dotyczące certyfikacji Common Criteria znajdziesz pod poniższym linkiem:
<https://www.commoncriteriaportal.org/>

Blokada instalacji aplikacji	Jeśli włączona, nie będzie możliwości instalowania aplikacji na urządzeniu. Dostępność: Android, Apple, Windows Phone 8.1 / 10, urządzenia w trybie Device Owner
Powiadomienie, gdy instalacja aplikacji jest zablokowana	Możliwość ustawienia treści powiadomienia wyświetlanego, gdy użytkownik próbuje zainstalować zablokowaną aplikację. Domyślnie: Instalacja aplikacji jest niedozwolona. Dostępność: Android
Zezwól na debugowanie USB	Jeśli ustawione, zezwala na uruchomienie na urządzeniu trybu debugowania USB. Dostępne dla trybu Device Owner, Android Samsung z Enterprise SDK 3.0, dla Android Sony z Enterprise SDK od 5.0 oraz Windows Phone 8.1/10. USB debugging is blocked by default.
Blokada nieznanych źródeł	Uniemożliwia zmianę ustawień instalacji z nieznanych źródeł. Dostępność: tryb Device Owner, Android Samsung z Enterprise SDK 2.0 oraz Windows 10 Mobile
Wyłącz możliwość kontrolowania aplikacji	Jeśli włączona, użytkownicy nie będą mogli modyfikować aplikacji (odinstalować, zatrzymać działanie, wyczyścić dane aplikacji). Dostępność: Android Device Owner
Tworzenie kont za pomocą Google Play	Możliwość wyłączenia / włączenia tworzenia kont za pomocą Google Play Po ustawieniu blokady instalatora tworzenie kont za pomocą Google Play jest automatycznie wyłączane. Dostępność: właściciel urządzenia z Androidem
Zezwalaj na debugowanie USB na urządzeniach Windows 10 Mobile	Jeśli włączona, debugowanie USB można włączyć na urządzeniu. Dostępność: Windows 10 Mobile Debugowanie USB jest domyślnie blokowane.
Blokada nieznanych źródeł na urządzeniach Windows 10 Mobile	Jeśli ustawione, możliwość zmiany ustawienia nieznanych źródeł jest zablokowana. Dostępność: Windows 10 Mobile
Blokada ręcznej instalacji certyfikatu root	Jeśli włączona, nie będzie możliwości ręcznego zainstalowania certyfikatu głównego. Dostępność: Windows Phone 8.1/10
Wyłącz App Store	Blokuje dostęp do App Store Dostępność: iOS supervised
Blokuj interaktywną instalację profili	Jeśli włączona, uniemożliwia użytkownikowi interaktywną instalację profili konfiguracyjnych i certyfikatów Dostępność: iOS supervised

konfiguracji i certyfikatów	
--------------------------------	--

2.4.9 Ograniczenia aplikacji

Poniżej znajduje się lista ustawień dostępnych w zakładce **Ograniczenia aplikacji**.

Atrybut	Opis
Ograniczenia aplikacji	
Blokada nagrywania głosu w aplikacjach	Jeśli włączona, wyłącza możliwość korzystania z mikrofonu. Dostępność: urządzenia Android Samsung 4.x z Enterprise SDK, Windows Phone 8.1/10
Nie wymuszaj Google Play Protect	Skanowanie Google Play Protect w celu ochrony przed złośliwym oprogramowaniem jest domyślnie włączone. Ta opcja umożliwia wyłączenie skanowania. Wymaga najnowszej wersji Google Play services na Androidach 6.0, 7.0 z aktywnym profilem służbowym. Dostępność: Android
Blokada zmiany ustawień telefonu	Jeśli włączona, uniemożliwia przejście do ustawień telefonu. Dostępność: Android, tryb Device Owner
Blokada zmiany ustawień zegara	Jeśli włączona, uniemożliwia przejście do ustawień czasu na urządzeniu. Dostępność: Android Samsung z Enterprise SDK 3.0
Wymuszaj automatyczne ustawienie daty i godziny	Jeśli włączona, wymusza automatyczne ustawienia daty i godziny na urządzeniu. Dostępność: iOS supervised 12.0, tvOS 12.2
Blokada przeglądarki WWW	Jeśli włączona, uniemożliwia uruchomienia przeglądarki internetowej. Dostępność: Android, Apple, Windows Phone 8.1/10, tryb Device Owner
Wyłącz możliwość modyfikowania kont	Jeśli włączona, możliwość dodania, edycji lub usunięcia konta zostanie zablokowana Dostępność: tryb Device Owner oraz urządzenia iOS w trybie nadzorowania
Blokada zarządzania kontami użytkownika	Jeśli włączona, uniemożliwia tworzenie dodatkowych kont użytkowników. Dostępność: Android Samsung z Enterprise SDK od 4.0

Blokada tworzenie konta email	Jeśli włączona, uniemożliwia tworzenie kont e-mail na urządzeniu. Dostępność: Android (nie dostępne dla Android 5.0) oraz urządzenia Windows Phone 8.1/10
Wyłącz możliwość usuwania aplikacji systemowych z urządzenia	Jeśli włączona, niemożliwe będzie usunięcie aplikacji systemowych. Dostępność: iOS 11.0
Wyłącz AirDrop	Jeśli włączona, udostępnianie plików za pomocą usługi AirPrint będzie wyłączone. Dostępność: iOS supervised
Nie zezwalaj na udostępnianie zarządzanych dokumentów za pomocą AirDrop	Jeśli włączona, udostępnianie zarządzanych dokumentów za pomocą usługi AirPrint będzie wyłączone. Dostępność: iOS supervised
Nie zezwalaj na udostępnianie danych z niezarządzanych aplikacji	Jeśli włączona, udostępnianie danych z niezarządzanych aplikacji będzie niemożliwe. Dostępność: iOS
Wyłącz udostępnianie haseł za pomocą funkcji Airdrop Passwords	Jeśli włączona, niemożliwe będzie udostępnianie haseł między urządzeniami za pomocą funkcji AirDrop. Dostępność: iOS 12.0, macOS 10.14
Nie zezwalaj na udostępnianie danych z zarządzanych aplikacji	Jeśli włączona, udostępnianie danych z zarządzanych aplikacji będzie niemożliwe. Dostępność: iOS
Zezwalaj zarządzanym aplikacjom na zapis kontaktów w niezarządzanych kontach z kontaktami	Jeśli włączona, zarządzane aplikacje będą mogły zapisywać kontakty w niezarządzanych kontach. Dostępność: iOS 12.0
Zezwalaj niezarządzanym aplikacjom na czytanie z zarządzanych kont z kontaktami	Jeśli włączona, niezarządzane aplikacje będą mogły odczytywać kontakty z zarządzanych kont. Dostępność: iOS 12.0
Włącz ograniczenia 'Nie zezwalaj na udostępnianie danych z niezarządzanych/	Blokuje możliwość kopiowania danych z niezarządzanych i zarządzanych aplikacji Dostępność: iOS 15.0

zarządzanych aplikacji' dla funkcji kopiowania i wklejania	
Wyłącz autouzupełnianie haseł w aplikacjach	Jeśli włączona, hasła w aplikacjach nie będą automatycznie uzupełniane. Dostępność: iOS 12.0, macOS 10.14
Nie żądaj haseł z urządzeń w pobliżu	Jeśli włączona, hasło nie będzie żądane na urządzeniach w pobliżu. Dostępność: iOS 12.0, macOS 10.14, tvOS 12.0
Uwierzytelnij Face ID/Touch ID przed zezwoleniem na automatyczne wprowadzanie haseł lub danych karty kredytowej	Jeśli włączona, konieczne będzie uwierzytelnienie odciskiem palca lub zdjęciem twarzy przed użyciem opcji automatycznego uzupełniania haseł lub danych karty kredytowej. Dostępność: iOS 11.0
Blokuj iCloud Private Relay	Dostępność: iOS 15.0, macOS 12.0
Wyłącz iCloud Photo Library	Uniemożliwia dostęp do usługi iCloud Photo Library. Dostępność: iOS, macOS 10.12
Wyłącz usługę Apple Music	Uniemożliwia dostęp do usługi Apple Music. Dostępność: iOS supervised, macOS 10.12
Wyłącz tworzenie kopii zapasowej urządzenia w usłudze iCloud	Uniemożliwia tworzenie kopii zapasowej w chmurze (iCloud). Dostępność: iOS
Wyłącz synchronizowanie dokumentów z usługą iCloud	Możliwość wyłączenia synchronizacji dokumentów z usługą iCloud. Dostępność: iOS supervised, macOS 10.11
Wyłącz synchronizowanie pęku kluczy iCloud	Możliwość wyłączenia synchronizacji menadżera haseł w iCloud keychain (Apple iCloud Keychain). Dostępność: iOS supervised, macOS 10.12
Wyłącz synchronizację zakładki w macOS iCloud	Możliwość wyłączenia synchronizacji zakładek w macOS iCloud. Dostępność: macOS 10.12
Wyłącz usługi macOS iCloud Mail	Możliwość wyłączenia usługi macOS iCloud Mail. Dostępność: macOS 10.12

Wyłącz usługi macOS iCloud Calendar	Możliwość wyłączenia usługi macOS iCloud Calendar. Dostępność: macOS 10.12
Wyłącz usługi macOS iCloud Reminder	Możliwość wyłączenia usługi macOS iCloud Reminder. Dostępność: macOS 10.12
Wyłącz usługi macOS iCloud Address Book	Możliwość wyłączenia usługi macOS iCloud Address Book. Dostępność: macOS 10.12
Wyłącz usługi macOS iCloud Notes	Możliwość wyłączenia usługi macOS iCloud Notes. Dostępność: macOS 10.12
Wyłącz iTunes	Dostępność: iOS
Wyłącz udostępnianie plików przez iTunes	Możliwość wyłączenia udostępniania plików przez iTunes. Dostępność: macOS 10.13
Wymuszaj na użytkownika wprowadzenie hasła iTunes dla każdej transakcji	Dostępność: iOS
Wyłącz zwracanie przez Spotlight wyszukiwań w internecie	Jeśli włączona, usługa Spotlight nie będzie zwracać wyników wyszukiwania przez Internet. Dostępność: iOS supervised, macOS 10.11
Wyłącz parowanie Apple TV z aplikacją Remote lub widżetem Control Center	Jeśli włączona, Apple TV nie będzie łączyć się z aplikacją Remote lub widżetem Control Center. Dostępność: tvOS 10.12
Maksymalny dozwolony poziom zawartości filmu na urządzeniu	Poziomy według ocen systemu MPAA. Dostępne opcje: Żadne, Wszystkie, G, PG, PG-13, R, NC-17. Dostępność: iOS 11.3, tvOS 11.3
Maksymalny dozwolony poziom zawartości programów TV na urządzeniu	Poziomy według ocen systemu TV Parental Guidelines. Dostępne opcje: Żadne, Wszystkie, TV-Y, TV-Y7, TV-G, TV-PG, TV-14, TV-MA. Dostępność: iOS 11.3, tvOS 11.3
Maksymalny dozwolony poziom zawartości aplikacji na urządzeniu	Możliwość ustawienia zakresu wiekowego: od 4, 9, 12 lub 17 lat. Możesz również wybrać opcję Wszystkie lub Żadne. Dostępność: iOS 11.3, tvOS 11.3
Wyłącz opcję Znajdź moje urządzenie w aplikacji Lokalizator	Jeśli ustawione, opcja Znajdź moje urządzenie zostanie wyłączona. Dostępność: iOS 13.0

Wyłącz opcję Znajdź moich przyjaciół w aplikacji Lokalizator	Jeśli ustawione, opcja Znajdź moich przyjaciół zostanie wyłączona. Dostępność: iOS 13.0
Wyłącz zmiany w Znajdź moich znajomych	Dostępność: iOS supervised
Wyłącz kontynuowanie rozpoczętej czynności na innym urządzeniu	Jeśli ustawione, nie będzie można kontynuować rozpoczętej czynności na innym urządzeniu. Dostępność: iOS, macOS 10.15
Blokada wykorzystania danych lokalizacyjnych przez wyszukiwarę	Jeśli włączona, wyszukiwanie nie będzie używać informacji o lokalizacji. Dostępność: Windows Phone 8.1/10
Blokada funkcji Zapisz jako w Microsoft Office	Jeśli włączona, blokuje opcję "Zapisz jako" w Microsoft Office. Dostępność: Windows Phone 8.1
Blokada funkcji udostępniania plików w Microsoft Office	Jeśli włączona, blokuje opcję "Udostępnij plik" w Microsoft Office. Dostępność: Windows Phone 8.1
Wyłącz możliwość modyfikowania kont dla urządzeń Apple	Jeśli ustawione, możliwość dodania, edycji lub usunięcia konta zostanie zablokowana Dostępność: urządzenia iOS w trybie Supervised
Zezwalaj na korzystanie z TLS 1.0/1.1 w Safari	Jeśli ustawione, możliwe będzie korzystanie z TLS 1.0 / 1.1 w przeglądarce Safari. Dostępność: iOS 13.4, macOS 10.15
Zablokuj użytkownikowi możliwość dodawania miniaplikacji App Clips	Jeśli ustawione, użytkownik nie może tworzyć żadnych klipów aplikacji Dostępność: urządzenia iOS w trybie Supervised
Ogranicz spersonalizowane reklamy Apple	Umożliwia ograniczenie wyświetlania reklam opartych na zainteresowaniach Dostępność: iOS
Wyłącz możliwość odinstalowywania aplikacji	Blokuje opcję usuwania zarządzanych aplikacji Dostępność: iOS 14.0, tvOS 14.0
Włącz możliwość przywrócenia kopii zapasowej z konta Google	Przywracanie danych z kont prywatnych jest domyślnie wyłączone, zaznacz tę opcję, aby ją włączyć. Dostępność: Android 10.0+
Blokuj zaufanie aplikacjom firmowym	Usuwa przycisk Trust Enterprise Developer w Ustawienia > Ogólne > Profile i zarządzanie urządzeniami

	Dostępność: iOS
Blokuj zakupy w aplikacji	Dostępność: iOS
Blokuj powiadomienia Passbook na zablokowanym ekranie	Dostępność: iOS
Wymuszaj ograniczenie śledzenia reklam	Dostępność: iOS
Blokuj autouzupełnianie w Safari	Dostępność: iOS supervised, macOS
Blokuj JavaScript w Safari	Dostępność: iOS
Blokuj wyskakujące okna w Safari	Dostępność: iOS
Włącz w Safari ostrzeżenia o oszustwach	Dostępność: iOS
Akceptowane cookies przez Safari	Możliwe opcje: Zawsze, Nigdy, Z odwiedzanych stron
Wyłącz centrum gier	Dostępność: iOS supervised, macOS 10.13
Wyłącz dodawanie znajomych do Game Center	Dostępność: iOS supervised, macOS
Blokuj gry wieloosobowe	Dostępność: iOS supervised, macOS 10.13
Blokuj usuwanie aplikacji	Dostępność: iOS
Zapobiegaj automatycznemu pobieraniu aplikacji zakupionych na innym urządzeniu	Dostępność: iOS
Usuń kartę Księgarnia z aplikacji Książki	Dostępność: iOS

Wyłącz pobieranie multimediiów Apple Books oznaczonych jako erotyka	Dostępność: iOS, macOS, tvOS
Wyłącz aplikację iMessage	Dostępność: iOS
Ukrywaj niecenzuralną muzykę lub materiały wideo zakupione w iTunes Store	Dostępność: iOS, macOS, tvOS 11.3
Wyłącz łączenie się z dyskami sieciowymi w aplikacji Pliki	Dostępność: iOS 13.1
Wyłącz łączenie się z dowolnymi podłączonymi urządzeniami USB w aplikacji Pliki	Dostępność: iOS 13.1
Wyłącz aplikację News	Dostępność: iOS supervised
Wyłącz podcasty	Dostępność: iOS supervised, macOS
Wyłącz Apple Music Radio	Dostępność: iOS supervised
Wyłącz Shared Photo Stream	Dostępność: iOS
Ukryj aplikację FaceTime	Dostępność: iOS supervised
Wymuś automatyczne dołączanie do klasy	Dostępność: iOS supervised, macOS 10.14.4
Wymagaj prośby o pozwolenie na opuszczenie zajęć	Dostępność: iOS supervised, macOS 10.14.4
Zezwól na blokowanie aplikacji lub urządzenia bez monitu	Dostępność: iOS supervised, macOS 10.14.4
Zezwól na nieoczekiwaną	Dostępność: iOS supervised, macOS 10.14.4

obserwację ekranu w klasie	
Wyłącz przechwytywanie treści na urządzeniu	Dostępność: Android Device Owner
Wyłącz sugestie dotyczące treści na urządzeniu	Dostępność: Android Device Owner

2.4.10 Polityka aplikacji

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka aplikacji**.

Atrybut	Opis
Polityka aplikacji	
Polityka aplikacji na urządzeniu Android	Ogólne ustawienie polityki haseł aplikacji. • Nie pytaj o hasło – jeśli ustawione, hasło będzie wymagane tylko dla aplikacji wymienionych na liście "Polityki haseł aplikacji" • Pytaj o kod blokady – jeśli ustawione, kod blokady będzie wymagany dla wszystkich aplikacji (poza wymienionymi na liście "Polityki haseł aplikacji") • Pytaj o hasło administratora – jeśli zostanie ustawione, hasło administratora będzie wymagane dla wszystkich aplikacji (poza wymienionymi na liście "Polityki haseł aplikacji") Dostępność: Urządzenia z Androidem Wartość domyślna: "Nie pytaj o hasło"
Lista aplikacji Android	Wprowadź nazwę pakietu, aby ustawić ograniczenia dla określonych aplikacji: • Blokuj • Blokada deinstalacji - nie można odinstalować aplikacji • Blokuj wymuszenie zatrzymania – jeśli ustawione, użytkownik nie będzie mógł zamknąć aplikacji za pomocą opcji Wymuś zatrzymanie • Blokuj czyszczenie danych - jeśli ustawione, użytkownik nie będzie mógł wyczyścić danych aplikacji za pomocą opcji Wyczyść dane • Polityka haseł - możliwe wybory - Nie pytaj o hasło / Pytaj o kod blokady / Pytaj o hasło administratora

Czas wygaśnięcia hasła aplikacji	Okres, po którym pojawi się na urządzeniu monit o wygaśnięciu hasła. Można ustawić na 1/5/10/15 minut. Dostępność: urządzenia z systemem Android Wartość domyślna: 5 minut
Powiadomienie gdy aplikacja jest zablokowana hasłem	Konfigurowalne powiadomienie wyświetlane na urządzeniu, gdy aplikacja jest zablokowana hasłem. Domyślnie: Wprowadź hasło FAMOC. Dostępność: urządzenia z systemem Android
Powiadomienie gdy aplikacja jest zablokowana	Konfigurowalne powiadomienie wyświetlane na urządzeniu, gdy aplikacja jest zablokowana. Domyślnie: Aplikacja została zablokowana. Dostępność: urządzenia z systemem Android
Polityka aplikacji Windows Phone	Można ustawić na: • "Blokuj aplikacje z listy" - zablokuje wszystkie aplikacje zdefiniowane w sekcji "Dozwolone/Blokowane" • "Zezwalaj na aplikacje z listy" - zezwoli na wszystkie aplikacje zdefiniowane w sekcji "Dozwolone/Blokowane"
Polityka aplikacji Apple	Można ustawić na: • "Blokuj aplikacje z listy" - zablokuje wszystkie aplikacje zdefiniowane w sekcji "Dozwolone/Blokowane" • "Zezwalaj na aplikacje z listy" - zezwoli na wszystkie aplikacje zdefiniowane w sekcji "Dozwolone/Blokowane" Możliwe jest również blokowanie webclipów, aby zablokować wszystkie webclipy, wpisz <code>com.apple.webapp</code> Dostępność: urządzenia z systemem iOS w trybie nadzorowanym
Polityka aplikacji w trybie Device Owner	Można ustawić na: • "Brak polityki aplikacji" - nie wprowadzi żadnych zmian we wszystkich aplikacjach zdefiniowanych w sekcji "Dozwolone/Blokowane" • "Blokuj aplikacje z listy" - zablokuje wszystkie aplikacje zdefiniowane w sekcji "Dozwolone/Blokowane" • "Zezwalaj tylko na aplikacje z listy" - zezwoli na wszystkie aplikacje zdefiniowane w sekcji "Dozwolone/Blokowane" Dostępność: Urządzenia w trybie Device Owner
Global polityka uprawnień aplikacji w trybie Device Owner	Można ustawić na: • "Zarządzane przez użytkownika" - pozwala użytkownikowi wybrać, które uprawnienia są zabronione lub dozwolone • "Zezwalaj" - zezwoli na wszystkie uprawnienia dla aplikacji zdefiniowanych w sekcji "Wyjątki uprawnień aplikacji" • "Blokuj" - zablokuje wszystkie uprawnienia dla aplikacji zdefiniowanych w sekcji "Wyjątki uprawnień aplikacji" Dostępność: Urządzenia w trybie Device Owner

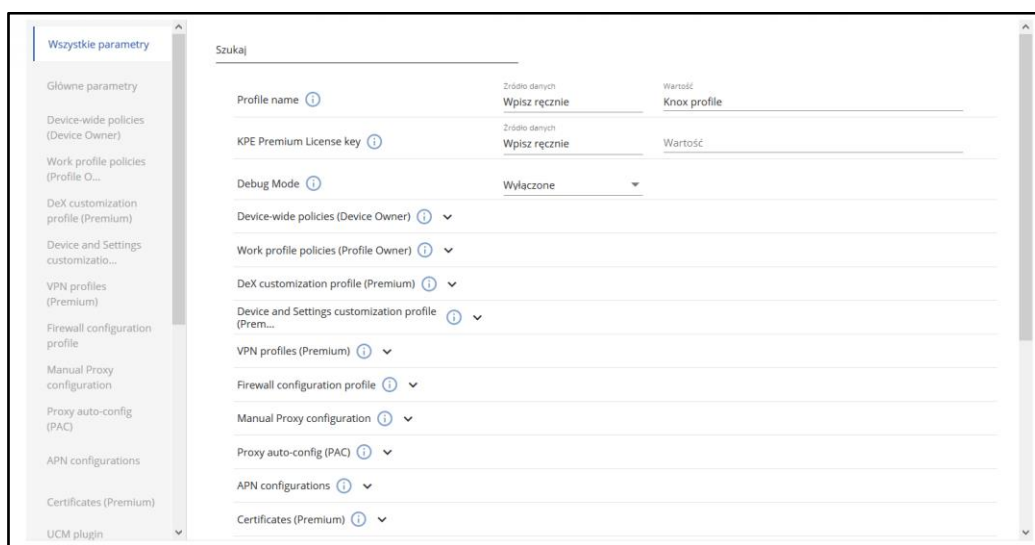
Ustawienia automatycznej aktualizacji aplikacji z zarządzanego Google Play	Można ustawić na: • Włącz automatyczne aktualizacje • Włącz automatyczne aktualizacje tylko wtedy, gdy urządzenie jest podłączone do Wi-Fi • Zezwalaj użytkownikowi urządzenia na konfigurowanie zasad aktualizacji aplikacji • Wyłącz automatyczne aktualizacje Dostępność: Android i urządzenia w trybie DO z zarządzanym Sklepem Google Play
Dostępność aplikacji w sklepie MGP	Ta opcja określa dostępność aplikacji w Managed Google Store. Można ustawić na: • Tylko włączone aplikacje (domyślnie) – dostępne będą tylko aplikacje włączone i zaakceptowane w Zarządzanym Sklepie Google Play przez FAMOC • Wszystkie aplikacje z Google Play – wszystkie aplikacje są wyświetlane w Zarządzanym Sklepie Google Play i można je instalować

2.4.11 Samsung KSP

Knox Service Plugin (KSP) to rozwiązanie umożliwiające konfigurowanie polityk i zarządzanie urządzeniami mobilnymi obsługującymi platformę Samsung Knox dla przedsiębiorstw (KPE). Procedura konfiguracji KSP opisana jest w osobnym dokumencie dostępnym [tutaj](#).

Ustawienia KSP są częścią sekcji Opcje bezpieczeństwa w szablonie polityk. Aby użyć ustawień KSP w swojej polityce, kliknij opcję Włącz Samsung KNOX Service Plugin. Następnie kliknij Edytuj konfigurację.

KSP zapewnia szereg konfigurowalnych parametrów. Aby ułatwić nawigację po ustawieniach, możesz skorzystać z pola wyszukiwania.



Listę wszystkich dostępnych parametrów można znaleźć tutaj:

<https://docs.samsungknox.com/admin/knox-service-plugin/release-notes.htm>

2.5 Zaawansowane

W zakładce ustawień zaawansowanych można ustawić następujące parametry:

Atrybut	Opis
Zaawansowane ustawienia polityk	
Rodzaj potwierdzania operacji dla Agenta Bazowego	Tryb potwierdzenia Agenta Bazowego: • Tryb cichy oznacza, że administrator może skonfigurować różne opcje bez przeszkadzania użytkownikowi. • Tryb informowania oznacza, że użytkownik otrzyma powiadomienie za każdym razem, gdy administrator chce podjąć działanie. • Tryb potwierdzania wymaga potwierdzenia użytkownika za każdym razem, gdy administrator chce podjąć działanie Wartość domyślna: Tryb cichy
Hasło administratora do aplikacji FAMOC Base Agent	Ochrona hasłem dla ustawień agenta bazowego na urządzeniu (jeśli pozostawiona pusta, nie jest używane żadne hasło) Wartość domyślna: 12345
Ilość zapamiętanych sesji Monitora urządzenia	Określa, ile sesji Monitora urządzenia ma być przechowywanych przez FAMOC (1-10) Wartość domyślna: 5
Ilość archiwalnych sesji Monitora urządzenia:	Określa, ile sesji Monitora urządzenia ma być przechowywanych w logach (10-150) Default value: 20
Dane raportowane w sesji Monitora urządzenia	Wybierz, które dane będą raportowane przez monitor użytkownika. Wartość domyślna: Wszystkie (możliwe wybory: parametry podstawowe; aplikacje; Bluetooth; dyski; punkty dostępu; certyfikaty; administratorzy urządzeń; konta na urządzeniu; aktualizacje oprogramowania; karty SIM)
Interwał synchronizacji czasu	Ustawia, jak często zegar systemowy urządzenia S60 jest zsynchronizowany z serwerem Network Time Protocol Wartość domyślna: Wyłączony
Informowanie o zmianie karty SIM (np. podczas kradzieży telefonu)	Tak/Nie Wartość domyślna: Nie

Limit urządzeń na użytkownika	Liczba urządzeń, które użytkownik może dodać za pomocą strony startowej, gdy ustawiana jest opcja autoryzacji użytkownika. Jeśli limit zostanie przekroczony, użytkownik nie może dodawać żadnego innego urządzenia do systemu za pomocą strony startowej.
Nazwa organizacji wyświetlana na urządzeniu	Wprowadzona nazwa zostanie wyświetlona na ekranie jako - Twoim urządzeniem zarządza (nazwa firmy)
Pokaż drugą linię w nagłówku FAMOC Base Agent	Wybierz, czy chcesz, aby dodatkowe informacje o nazwie organizacji zarządzającej urządzeniem były wyświetlane w agencie bazowym FAMOC.
Wartość drugiej linii w nagłówku FAMOC Base Agent	Tekst wyświetlany w polu opisanym powyżej.

Ciągłe raportowanie i ostrzeganie o parametrach

W tej sekcji możesz zdefiniować, które parametry baterii będą raportowane w czasie rzeczywistym. Możesz włączyć raportowanie ciągłe lub szczytowe. Jeśli stan baterii przekroczy określony próg lub status, w konsoli zarządzania FAMOC pojawi się alert.

Dostępne parametry są wymienione poniżej:

- Stan baterii - gdy raportowana wartość różni się od podanej (np. określono: dobry, zaraportowane: przegrzanie)
- Poziom naładowania baterii - gdy raportowana wartość jest niższa niż określona 10%-50%
- Temperatura akumulatora - gdy raportowana wartość jest wyższa niż określone 20-100 stopni Celsjusza
- Napięcie akumulatora - gdy raportowana wartość jest wyższa niż podana 2V-10V
- Stan ładowarki - gdy raportowany stan różni się od podanego (np. określony: Podłączony, raportowany: Brak połączenia)
- Niski poziom baterii - gdy zgłaszana wartość jest równa podanej
- Pamięć RAM Wolna - gdy raportowana wartość jest niższa niż określona (10-50%)
- Siła sygnału - gdy raportowana wartość jest niższa niż określona (np. określona: -80 dBm, raportowana: -107 dBm)

Szczegóły urządzenia w agencie bazowym

Administrator może dodać niestandardowe pola, które będą wyświetlane na karcie **Informacje o urządzeniu**.

Rysunek 21 Pola szczegółów urządzenia

Ustawienia kopii zapasowej

W tej sekcji możliwe jest ustawienie synchronizacji wszystkich kontaktów lub synchronizację danych tylko w grupach, których członkiem jest użytkownik. W przypadku tej drugiej opcji administrator może określić dodatkowe grupy, z których będą zsynchronizowane kontakty. Aby dodać grupy użytkowników do synchronizacji danych kontaktowych, użyj przycisku Wybierz. Możesz także ustawić interwał synchronizacji kontaktów codziennie, co tydzień lub co miesiąc.

Nazwa grupy	Liczba użytkowników	Przypisani użytkownicy	
Harvey Group	1	Harvey Specter	X
Mike Group	3	Mike Ross, Mike Bird, ff.michalk@outlook.com	X

Rysunek 22 Ustawienia synchronizacji kontaktów

Polityka kopii zapasowej

W tej sekcji można włączyć ustawienia reguł tworzenia kopii zapasowych, takie jak:

- **Ustawienia elementów kopii zapasowej** - które elementy będą zawarte w zasadach polityki backupu (kontakty, kalendarz, sms, foldery - na podstawie platformy).
- **Harmonogram kopii zapasowej** - ustawia częstotliwość synchronizacji danych (codziennie/co tydzień/co miesiąc/co X dni). Pod przyciskiem **Dodaj przykładowe**

FAMOC zapewnia predefiniowane wzorce tworzenia kopii zapasowych, np. raz w tygodniu w poniedziałek lub pierwszego dnia każdego miesiąca.

Zaznaczenie pola wyboru **Włącz usługi kopii zapasowych** aktywuje polityki tworzenia kopii zapasowych. Następnie **Agent kopii zapasowej** zostanie zainstalowany wraz z politykami, a ustawienia tworzenia kopii zapasowych zostaną zastosowane.

Rysunek 23 Ustawienia polityki kopii zapasowej

Polityka monitora użycia

Ta sekcja umożliwia ustawienie monitorowania użytkownika, w tym:

- Raportowanie przesyłu danych za pomocą WIFI
- Raportowanie przesyłu danych za pomocą GPRS
- Zgłaszanie treści SMS
- Raportowanie typu połączenia

Zaznaczenie pola wyboru **Włącz monitor użycia** aktywuje polityki użytkownika. W takim przypadku na urządzeniu zostanie zainstalowany Monitor użycia z uwzględnieniem adekwatnych polityk.

Atrybut	Opis
Ustawienia polityki monitora użycia	
Włącz monitor użycia	Jeśli ta opcja jest zaznaczona, Monitor użycia zostanie zainstalowany wraz z polityką. Wartość domyślna: niezaznaczona.

Raportuj dane po restarcie urządzenia	Jeśli zostanie ustawiony, Monitor użycia będzie zbierać i wysyłać dane po ponownym uruchomieniu urządzenia.
Raportuj użycie danych po WIFI co:	Interwał w raportowaniu danych WIFI (Nie zgłaszaj/1 dzień/3 dni/1 tydzień/2 tygodnie/1 miesiąc/3 miesiące). Wartość domyślna: 1 miesiąc.
Raportuj użycie danych po GPRS co:	Interwał w raportowaniu danych GPRS (Nie zgłaszaj/1 dzień/3 dni/1 tydzień/2 tygodnie/1 miesiąc/3 miesiące). Wartość domyślna: 1 miesiąc.
Raportuj treść SMS	Jeśli zostanie ustawione, treść SMS będzie raportowana. Wartość domyślna: niezaznaczona.
Raportuj stan urządzenia	Jeśli jest ustawione, raportuje stan urządzenia. Wartość domyślna: niezaznaczona.
Raportuj czas odblokowania/zablokowania ekranu	Zaznacz, aby zbierać informacje o czasie odblokowania ekranu.
Raportuj użycie aplikacji⁴	Jeśli jest ustawione, raportuje użycie aplikacji. Wartość domyślna: niezaznaczona.
Raportuj historię przeglądarki	Jeśli jest ustawione, raportuje historię przeglądarki. Wartość domyślna: niezaznaczona.
Raportuj rozszerzone parametry co:	Interwał raportowania stanu urządzenia, użycia aplikacji i historii przeglądarki (Nie zgłaszaj/15 minut/30 minut/1 godzina/6 godzin/1 dzień/3 dni/1 tydzień/2 tygodnie/1 miesiąc) Wartość domyślna: 1 dzień.
Pozwalaj użytkownikowi wybrać typ rozmowy	Jeśli wybrano Zezwalaj , przy wykonywaniu połączenia użytkownik zostanie poproszony o wybranie typu. Lista typów połączeń może być zmieniana. Domyślnie dostępne są dwa typy: prywatne/firmowe. Wartość domyślna: nie zezwalaj.

⁴ W przypadku systemu Android 6.0 lub nowszego raportowanie użycia aplikacji wymaga włączenia na urządzeniu usługi Application Monitor Service.

Ustawienia polityki monitora użycia	
Włącz monitor użycia:	☒
Raportuj dane po restarcie urządzenia:	☒
Ustawienia danych pakietowych	
Raportuj użycie danych po WIFI co:	1 dzień
Raportuj użycie danych po GPRS co:	1 dzień
Ustawienia wiadomości	
Raportuj treść SMS:	☒
Ustawienia rozszerzonego raportowania	
Raportuj stan urządzenia:	☒
Raportuj użycie aplikacji:	☒
Raportuj historię przeglądarki:	☒
Raportuj rozszerzone parametry co:	1 dzień
Ustawienia raportowania rozmowy głosowej	
Pozwalaj użytkownikowi wybrać typ rozmowy:	Nie pozwalaj

Rysunek 24 Ustawienia polityki monitora użycia

3. Szablony polityk BYOD/WPC

Polityki BYOD/WPC nieznacznie różnią się od zasad w pełni zarządzanych. W takim podejściu większość ustawień wpłynie tylko na kontener profilu pracy na urządzeniu. Wszystkie komponenty, ograniczenia i włączone aplikacje będą działać tylko w kontenerze. Prywatna część urządzenia będzie działać zgodnie z ustawieniami użytkowników.

3.1 Ustawienia podstawowe

Aby dodać ogólny szablon polityk, podaj nazwę i ustaw priorytet.

Atrybut	Opis
Ustawienia podstawowe	
Nazwa szablonu	Wprowadź nazwę polityki (maks. 100 znaków)
Ustaw priorytet	Określ pozycję na liście szablonów
Przeinstaluj Base Agenta automatycznie	Po pojawieniu się w systemie nowej wersji programu Base Agent zostanie ona automatycznie ponownie zainstalowana na urządzeniach (polityka zostanie ustawiona jako nieaktualna). Wartość domyślna: niezaznaczone.
Odinstaluj niezgodne elementy polityki automatycznie	Jeśli ta opcja jest zaznaczona, niepasujące elementy z bieżącej polityki zostaną odinstalowane, jeśli urządzenie zostanie przypisane do innej polityki. Wartość domyślna: niezaznaczone.

Włącz Samsung Premium API	Aby aktywować Samsung Premium API w polityce, należy zaznaczyć tę opcję ⁵ . Należy również podać odpowiedni klucz licencyjny. Wartość domyślna: niezaznaczone.
Licencja premium	Licencja Samsung Premium może być dodana/zmieniona /usunięta przy użyciu ikon plus/minus obok pola klucza licencyjnego.
Włącz atestację Samsung	Jeśli ta opcja jest zaznaczona, dodatkowa operacja dla atestacji Samsung KNOX zostanie dodana do kolejki i sprawdzi integralność oprogramowania urządzenia przed utworzeniem kontenera KNOX. Wartość domyślna: niezaznaczone.
Oznacz urządzenie jako wyczyszczone przy wykrytym odinstalowaniu Agentu Bazowego	Jeśli ta opcja jest zaznaczona, urządzenie zostanie oznaczone w konsoli FAMOC jako wyczyszczone w przypadku odinstalowania Agentu Bazowego. Wartość domyślna: niezaznaczone.
Włącz usługi zdalnego pulpitu	Jeśli ta opcja jest zaznaczona, Zdalny dostęp zostanie zainstalowany wraz z polityką. Wartość domyślna: niezaznaczone.
Włącz usługi lokalizacyjne	Jeśli ta opcja jest zaznaczona, Monitor lokalizacji zostanie zainstalowany wraz z polityką. Wartość domyślna: niezaznaczone.
Wymuszaj włączenie usługi monitorowania aplikacji	Po ustawieniu dodatkowa operacja zawarta w ogólnej polityce o nazwie "Włącz usługi monitorowania aplikacji" zostanie dodana do kolejki i wysłana do urządzenia z prośbą o włączenie przez użytkownika Usługi dostępności FAMOC.
Ignoruj optymalizację zużycia baterii dla Monitora lokalizacji i Monitora użycia	Po ustawieniu, do kolejki zostanie dodana dodatkowa operacja zawarta w polityce ogólnej, o nazwie „Włącz usługę monitorowania aplikacji” i wysłana do urządzenia z prośbą o włączenie usługi dostępności FAMOC.
Raportuj dodatkowe informacje o aplikacjach (rozmiar aplikacji, rozmiar pamięci podręcznej, rozmiar danych)	Wybierz, aby zebrać dodatkowe dane o aplikacjach
Raportowane aplikacje	Możliwe opcje: • Raportuj wszystkie aplikacje

⁵ Możesz przeczytać więcej o zaletach oferowanych przez KPE Premium tutaj: [Knox Platform for Enterprise | Advanced mobile security management](#)

- Raportuj tylko aplikacje zarządzane

Ustawienia podstawowe

Nazwa szablonu:

Ustaw priorytet:

Przeinstaluj Base Agent automatycznie: ☐

Odinstaluj niezgodne elementy polityki automatycznie: ☐

Włącz Samsung Premium API: ☒

Licencja premium: - - - - - +

Włącz atestację Samsung: ☐

Włącz atestację Safetynet: ☐

Oznacz urządzenie jako wyczyszczone przy wykryciu odinstalowania Agent Bazowego: ☐

Włącz usługi zdalnego pulpitu: ☐

Włącz usługi lokalizacyjne: ☐

Wymuszaj włączenie usługi monitorowania aplikacji: ☐

Ignoruj optymalizację zużycia baterii dla Monitora lokalizacji i Monitora użycia *: ☐

Rysunek 25 Zakładka ustawień podstawowych

3.1.1. Ustawienia harmonogramów

Poniżej znajduje się lista parametrów ustawień harmonogramów polityk.

Atrybut	Opis
Ustawienia harmonogramów	
Interwał synchronizacji w szczycie	Interwał połączenia z serwerem Base Agent: 5 min./15 min./30 min./1 g./4 g./12 g./Raz dziennie/Raz w tygodniu/Raz w miesiącu Wartość domyślna: raz dziennie
Dni szczytu	Dni tygodnia, w trakcie których Agent Bazowy raportuje do serwera FAMOC Wartość domyślna: od poniedziałku do piątku
Początek szczytu	O której godzinie w dniach szczytu powinien zacząć raportowanie agent podstawowy Wartość domyślna: 8:00
Koniec szczytu	O której godzinie w dniach szczytu powinien zakończyć raportowanie agent podstawowy Wartość domyślna: 16:00
Interwał sesji Monitora Urządzenia	Ustawia interwał sesji Monitora Urządzenia: Wyłączony/Co godzinę, 4 razy dziennie/Codziennie/Raz w tygodniu/Raz w miesiącu Wartość domyślna: Codziennie
Informowanie o nieaktywności urządzenia	Ostrzeżenie o bezczynności agenta bazowego po: 1-5 dniach/tygodniu/miesiącu/3 miesiącach. Jeśli agent bazowy nie połączy się z serwerem w tym okresie, FAMOC wygeneruje alert z trzema możliwymi opcjami reakcji: • Usuń urządzenie z FAMOC

	• Zainstaluj ponownie program Base Agent • Oznacz urządzenie jako skradzione Wartość domyślna: po tygodniu
Wyczyść urządzenie przy przekroczonej nieaktywności	Jeśli ta opcja jest zaznaczona, a agent bazowy nie zgłasza się do serwera w określonym czasie, oprócz wygenerowanego alertu urządzenie zostanie wyczyszczone.
Oznacz urządzenie jako wyczyszczone przy przekroczonej nieaktywności	W przypadku przekroczenia czasu zgłoszenia się urządzenia do serwera, zostanie ono oznaczone w konsoli FAMOC jako wyczyszczone.

Ustawienia harmonogramów

Interwał synchronizacji w szczycie:

Dni szczytu: ☒ Poniedziałek ☒ Wtorek ☒ Środa ☒ Czwartek ☒ Piątek ☐ Sobota ☐ Niedziela

Początek szczytu:

Koniec szczytu:

Interwał sesji Monitora urządzenia:

Informowanie o nieaktywności urządzenia:

Wyczyść urządzenie przy przekroczonej nieaktywności: ☐

Oznacz urządzenie jako wyczyszczone przy przekroczonej nieaktywności: ☐

Rysunek 26 Ogólne ustawienia polityk

3.2 Przypisane grupy

Każda polityka przypisana jest do określonych grup użytkowników lub grup urządzeń, dlatego każde urządzenie otrzymuje ustawienia polityk wstępnie zdefiniowane do przypisanej grupy. Urządzenia nienależące do żadnej grupy oraz grupy, które nie są przypisane do żadnej polityki, otrzymują politykę o najniższym priorytecie (polityka znajdująca się na dole listy). Urządzenia przypisane do kilku grup otrzymują politykę o wyższym priorytecie.

W zakładce **Grupy** administrator może przydzielać grupy do polityk. Aby wybrać grupę, kliknij przycisk **Dodaj grupę urządzeń** lub przycisk **Dodaj grupę użytkowników**. Zostanie wyświetlone okno z listą grup.

Grupy użytkowników

Lista przypisanych grup użytkowników Dodaj grupę użytkowników

Nazwa grupy	Liczba użytkowników	Przypisani użytkownicy

Rysunek 27 Zakładka Przypisane grupy

3.3 Elementy polityk

Oprócz ogólnych ustawień istnieje możliwość dodania konfiguracji i aplikacji do polityki.

Aby dodać konfigurację do polityki, kliknij przycisk **Wybierz konfigurację**. Pojawi się okno z listą konfiguracji.

Konfiguracja może być ustawiona dla:

- Szczytu – konfiguracja zostanie zastosowana w okresie szczytu
- Poza szczytem – konfiguracja zostanie zastosowana poza okresem szczytu
- Zawsze – konfiguracja będzie zawsze stosowana

Za każdym razem, gdy urządzenie łączy się z serwerem, sprawdza, czy zastosowana jest odpowiednia polityka, a jeśli potrzebna jest zmiana (np. zakończył się okres szczytu, a aktualnie stosowana konfiguracja dotyczy tylko tego okresu), stara konfiguracja jest usuwana, a zastosowana jest odpowiednia. Polityki oparte na czasie mogą być stosowane tylko na urządzeniach z systemem iOS.

Aby dodać aplikację, kliknij przycisk **Wybierz aplikację**. Pojawi się okno z listą aplikacji. Wybrane aplikacje zostaną zainstalowane podczas przypisywania polityk do urządzenia. Po zmianie polityk przypisanych do urządzenia zastosowane zostaną nowe polityki i zainstalowana nowa lista aplikacji. Podczas wyboru aplikacji, można określić liczbę powtórzeń instalacji (w przypadku anulowania instalacji przez użytkownika, FAMOC ponowi operację). Możliwe opcje:

- Instalacja obowiązkowa (opcja domyślna) - jeśli instalacja zostanie anulowana, będzie powtarzana co dzień.
- Jedna próba instalacji - jeśli instalacja zostanie anulowana, nie będzie ponawiana.
- Kilka prób instalacji - instalacja będzie ponawiana określoną liczbę razy.

Elementy polityki można ustawić w niestandardowej kolejności instalacji, używając strzałek w dół/w górę w kolumnie **Kolejność**.

Domyślnie każdy element jest instalowany w sekwencji (następny element rozpoczyna się po pomyślnym zainstalowaniu poprzedniego). Można jednak zaznaczyć element jako niezależny (kolumna **Niezależny**), co oznacza, że kolejna akcja rozpoczyna się niezależnie od poprzedniej, nie czekając na raport z powodzeniem.

Zaznacz opcję **Ignoruj błąd**, aby wykonać następną akcję, jeśli poprzednia zakończyła się niepowodzeniem.

Elementy polityki		Wybierz aplikację Wybierz konfigurację			
Nazwa elementu	Akcja	Ignoruj błąd	Niezależny	Kolejność	
Require 4 chars lock code on Android	Polityka szczytu: Zawsze ▾	☐	☐	↓	×
Tapeta FF 1080p	Polityka szczytu: Zawsze ▾	☐	☐	↑	×

Rysunek 28 Elementy polityki

3.4 Opcje bezpieczeństwa na urządzeniu

Ograniczenia na całym urządzeniu stosują się do ogólnego działania urządzenia.

Atrybut	Opis
Polityka czyszczenia danych	
Czyszczenie pamięci telefonu po wykryciu zmiany karty SIM	Jeśli ustawione, czyszczenie zostanie wykonane po wykryciu zmiany karty SIM
Czyszczenie pamięci telefonu na brak karty SIM	Jeśli ustawione, czyszczenie zostanie wykonane, gdy karta SIM nie zostanie wykryta. Opcja dostępna po ustawieniu pierwszej opcji (Czyszczenie danych przy zmianie karty SIM). OSTRZEŻENIE! Po zastosowaniu tej konfiguracji użytkownicy nie będą mogli korzystać z trybu samolotowego Androida, ponieważ spowoduje to wymazanie urządzenia.
Czyszczenie urządzenia po wykryciu rootowania	Jeśli ustawione, urządzenie zostanie wyczyszczone po wykryciu rootowania.
Ochrona przywracania do ustawień fabrycznych (FRP)	Factory Reset Protection to rozwiązanie, które umożliwia uruchomienie urządzenia po przywróceniu ustawień fabrycznych jedynie kontem Google, którym wcześniej zalogowano się na urządzeniu. Dostępne możliwości konfiguracji tego ustawienia: • wyłączona (opcja nie będzie dostępna) • odblokuj urządzenie aktywnym kontem (urządzenie można odblokować poprzednio używanym kontem) • odblokuj urządzenie za pomocą konta z listy (urządzenie można odblokować kontem z wprowadzonej listy - należy podać id użytkownika) • zdejmij blokadę FRP po wyczyszczeniu urządzenia (wyłącza blokadę po wyczyszczeniu urządzenia) Dostępność: Device Owner
Polityka sieci	
Blokada interfejsu Wi-Fi	Jeśli włączona niemożliwe będzie połączenie z Wi-Fi w ramach profilu służbowego
Blokada ręcznej konfiguracji WiFi	Jeśli włączona, nie będzie możliwości ręcznej konfiguracji Wi-Fi. Dostępność: Tryb Device Owner, urządzenia iOS w trybie nadzorowanym, Windows Phone 8.1 / 10

Zapobiegaj wyłączeniu Wi-Fi	Jeśli włączona, nie będzie możliwości wyłączenia Wi-Fi
Blokada interfejsu bluetooth	Jeśli włączona, na urządzeniu nie może być używana komunikacja Bluetooth.
Blokada danych pakietowych w roamingu	Możliwe opcje: - Nie blokuj - Wyłącz i zablokuj możliwość włączenia Dostępność: Android WPC 11+
Blokada rozmów wychodzących	Wyłącza połączenia wychodzące Dostępność: Android WPC 11+
Blokuj konfigurację Bluetooth	Blokuje możliwość zmiany ustawień Bluetooth Dostępność: Android WPC
Blokuj konfigurację udostępniania internetu	Blokuje możliwość zmiany ustawień tetheringu Dostępność: Android WPC 11+
Blokada konfiguracji sieci mobilnych	Blokuje możliwość zmiany ustawień Bluetooth Dostępność: Android WPC 11+
Blokada konfiguracji transmisji komórkowej	Blokuje możliwość konfiguracji Wireless Emergency Alerts (WEA), Amber Alerts Dostępność: Android WPC 11+
Wyłącz wiadomości SMS	Dostępność: Android WPC 11+
Polityka lokalizacji	
Zablokuj możliwość zmiany ustawień lokalizacji	Dostępność: Android WPC
Wyłącz możliwość udostępniania lokalizacji na urządzeniu	Dostępność: Android WPC 11+
Polityka aktualizacji	
Aktualizacje OTA dla urządzeń Zebra	Dostępność: Urządzenia Zebra z: Androidem 7.0 i nowszym, MX w wersji 9.2 lub nowszym
Polityka sprzętowa	
Blokada trybu awaryjnego	Dostępność: Android WPC 11+
Blokada trybu samolotowego	Dostępność: Android WPC 11+
Włącz tryb debugowania USB	Dostępność: Android BYOD oraz WPC

Blokada przechwytywania obrazu	Dostępność: Android WPC
Blokada przesyłania plików po USB	Dostępność: Android WPC 11+
Wyłącz możliwość montowania fizycznych nośników zewnętrznych	Dostępność: Android WPC
Polityka instalatora	
Blokada nieznanych źródeł	Dostępność: Android BYOD oraz WPC
Ograniczenia aplikacji	
Blokada nagrywania głosu w aplikacjach na urządzeniu	Jeśli jest ustawiony, mikrofon nie może być używany w urządzeniu. Dostępność: Android WPC
Wymuszaj automatyczne ustawienie daty i godziny	Dostępność: Android BYOD oraz WPC 11+
Polityka aplikacji na urządzeniu WPC	Można ustawić na: „Brak polityki aplikacji” – nie wprowadza żadnych zmian dla wszystkich aplikacji zdefiniowanych w sekcji „Zezwól na wpisy na liście / Odrzuć wpisy na liście” „Zezwalaj tylko aplikacjom z listy” – zezwoli na wszystkie aplikacje zdefiniowane w sekcji „Wpisy na białej/czarnej liście” „Blokuj aplikacje z listy” – blokuje wszystkie aplikacje zdefiniowane w sekcji „Wpisy na białej/czarnej liście” Dostępność: Android WPC
Wyłącz przechwytywanie treści na urządzeniu	Dostępność: Android WPC 11+
Wyłącz sugestie dotyczące treści na urządzeniu	Dostępność: Android WPC 11+

3.4 Opcje bezpieczeństwa w profilu do pracy

Poniższe ustawienia będą obowiązywać jedynie w ramach Profilu do pracy.

Parameter	Value
Polityka czyszczenia danych	

Usuń dane korporacyjne przy zmianie karty SIM	Jeśli ustawione, profil roboczy zostanie wyczyszczony po wykryciu zmiany karty SIM.
Usuń dane korporacyjne przy wykryciu braku karty SIM	Jeśli ustawione, profil roboczy zostanie wyczyszczony, gdy karta SIM nie zostanie wykryta. Opcja dostępna po ustawieniu pierwszej opcji (Wymazywanie danych przy zmianie karty SIM). OSTRZEŻENIE! Po zastosowaniu tej konfiguracji użytkownicy nie będą mogli korzystać z trybu samolotowego Androida, ponieważ spowoduje to wyczyszczenie urządzenia.
Usuń dane korporacyjne po wykryciu rootowania	Jeśli ustawione, profil roboczy zostanie wyczyszczony po wykryciu rootowania
Polityka sieci	
Wyłącz ustawienia VPN	Blokuje możliwość zmiany ustawień przez użytkownika Dostępność: Android BYOD i WPC
Blokada edycji zarządzanych sieci	Blokuje możliwość edycji ustawień WiFi zarządzanych przez FAMOC Dostępność: Android WPC 11 lub nowszy
Monitoruj listę zarządzanych konfiguracji Wifi	Monitoruje stan zarządzanych sieci i uruchamia alert w przypadku ich usunięcia (zapomniał na urządzeniu). Dostępność: Android BYOD i WPC
Polityka sprzętowa	
Wyłącz Siri	Możliwość wyłączenia asystenta Siri Dostępność: iOS, iPadOS
Wyłącz Siri kiedy urządzenie jest zablokowane	Zapobiega uruchamianiu Siri na zablokowanym urządzeniu Dostępność: iOS, iPadOS
Wyłącz połączenia z serwerami Siri na potrzeby dyktowania	Jeśli ta opcja jest ustawiona, połączenia z serwerami Siri na potrzeby dyktowania będą wyłączone Dostępność: iOS, iPadOS
Wyłącz połączenia z serwerami Siri na potrzeby tłumaczenia	Jeśli ustawione, połączenia z serwerami Siri na potrzeby tłumaczenia będą wyłączone Dostępność: iOS, iPadOS
Wyłącz automatyczne przesyłanie raportów diagnostycznych do Apple	Jeśli jest ustawiona, raport diagnostyczny nie będzie automatycznie przesyłany do Apple Dostępność: iOS, iPadOS
Wyłącz centrum kontroli na zablokowanym ekranie	Jeśli ustawione, Centrum kontroli nie pojawi się na ekranie blokady Dostępność: iOS, iPadOS

Nie pozwalaj na kopie zapasowe Enterprise books	Jeśli ustawione, kopia zapasowa książek Enterprise będzie wyłączona Dostępność: iOS, iPadOS
Nie pozwalaj na synchronizację metadanych Enterprise Book	Jeśli ta opcja jest ustawiona, synchronizacja metadanych Enterprise Book zostanie wyłączona Dostępność: iOS, iPadOS
Wyłącz podgląd historii powiadomień na zablokowanym ekranie	Jeśli ta opcja jest ustawiona, widok historii powiadomień na ekranie blokady będzie wyłączony Dostępność: iOS, iPadOS
Wyłącz podgląd dzisiejszych powiadomień na zablokowanym ekranie	Jeśli ta opcja jest ustawiona, widok historii powiadomień na ekranie blokady będzie wyłączony Dostępność: iOS, iPadOS
Wyłącz użycie iCloud przez zarządzane aplikacje	Jeśli ta opcja jest ustawiona, zarządzane aplikacje nie będą mogły korzystać z iCloud Dostępność: iOS, iPadOS
Wymuś użycie hasła do parowania na urządzeniach otrzymujących zadania z tego urządzenia	Jeśli ta opcja jest ustawiona, hasło parowania będzie wymagane, gdy urządzenie odbierze żądania AirPlay z tego urządzenia Dostępność: iOS, iPadOS
Wymuszenie szyfrowania kopii zapasowej	Wymusza szyfrowanie kopii zapasowej Dostępność: iOS, iPadOS
Wymuś rozpoznawanie nadgarstka na Apple Watch	Jeśli zaznaczone, wymusza na sparowanym zegarku Apple Watch korzystanie z funkcji wykrywania nadgarstka Dostępność: iOS, iPadOS
Wymuś ustawienie kodu blokady	Jeśli zaznaczone, wymusza użycie kodu blokady Dostępność: iOS, iPadOS
Polityka szyfrowania pamięci	
Szyfrowanie pamięci wewnętrznej	Jeśli ustawione, wymagane będzie szyfrowanie. Dostępność: Android
Polityka instalatora	
Blokada instalacji aplikacji	Jeśli ustawione, nie będzie możliwości instalowania aplikacji na urządzeniu. Dostępność: Android
Powiadomienie, gdy instalacja aplikacji jest zablokowana	Możesz ustawić powiadomienie, które pojawi się na urządzeniu, gdy użytkownik spróbuje zainstalować aplikację. Domyślnie: instalacja aplikacji jest niedozwolona Dostępność: Android
Tworzenie kont przez Google Play	Możliwość wyłączenia/włączenia tworzenia kont za pomocą Google Play Po ustawieniu blokady instalatora tworzenie kont za pomocą Google Play jest automatycznie wyłączane. Dostępność: Android

Ograniczenia aplikacji	
Blokada nagrywania głosu w aplikacjach	Jeśli jest ustawiona, mikrofon nie może być używany w urządzeniu. Dostępność: Android Samsung
Nie zezwalaj na udostępnianie zarządzanych dokumentów za pomocą AirDrop	Jeśli jest ustawiona, zarządzanych dokumentów nie można udostępniać za pomocą funkcji AirDrop. Dostępność: iOS, iPadOS
Nie zezwalaj na udostępnianie danych z niezarządzanych aplikacji	Jeśli ta opcja jest ustawiona, udostępnianie danych z niezarządzanych aplikacji będzie zabronione. Dostępność: Android BYOD i WPC, iOS, iPadOS
Nie zezwalaj na udostępnianie danych z zarządzanych aplikacji	Jeśli ta opcja jest ustawiona, udostępnianie danych z zarządzanych aplikacji będzie zabronione. Dostępność: iOS, iPadOS
Zezwalaj niezarządzanym aplikacjom na czytanie z zarządzanych kont z kontaktami	Dostępność: iOS, iPadOS
Włącz ograniczenia 'Nie zezwalaj na udostępnianie danych z niezarządzanych/zarządzanych aplikacji' dla funkcji kopiowania i wklejania	Dostępność: iOS 15, iPadOS 15
Wyłącz możliwości odinstalowywania aplikacji	Dostępność: iOS, iPadOS
Włącz w Safari ostrzeżenia o oszustwach	Dostępność: iOS, iPadOS
Polityka aplikacji	
Ustawienia automatycznej aktualizacji aplikacji z zarządzanego Google Play	Można ustawić na: • Włącz automatyczne aktualizacje • Włącz automatyczne aktualizacje tylko wtedy, gdy urządzenie jest połączone z Wi-Fi • Zezwól użytkownikowi urządzenia na skonfigurowanie zasad aktualizacji aplikacji • Wyłącz automatyczne aktualizacje Dostępność: Android BYOD i WPC
Dostępność aplikacji w sklepie MGP	Ta opcja określa dostępność aplikacji w Zarządzanym Sklepie Google Play. Można ustawić na: • Tylko włączone aplikacje (domyślnie) – dostępne będą tylko aplikacje włączone i zatwierdzone w zarządzanym Sklepie Google Play przez FAMOC

	Wszystkie aplikacje z Google Play – wszystkie aplikacje są wyświetlane w Zarządzanym Sklepie Google Play i można je instalować Dostępność: Android BYOD i WPC
Ograniczenia profilu do pracy	
Wyłączenie instalacji z nieznanymi źródłami	Zezwala lub blokuje możliwość instalowania aplikacji poprzez pliki .apk do profilu służbowego. Polityka nie będzie aktywna na urządzeniach z Androidem 5.0 (instalacja .apk jest zablokowana)
Blokada przechwytywania obrazu	Umożliwia zablokowanie przechwytywania ekranu w aplikacji, która działa w profilu do pracy, aby uniemożliwić udostępnianie danych tą metodą. Dostępność: Android, urządzenia Apple
Wyłącz możliwość modyfikowania kont	Blokuje możliwość dodawania, edytowania lub usuwania konta. Dostępność: Android BYOD i WPC
Blokada tworzenia konta email	Dostępność: tylko Samsung SDK
Blokada tworzenia konta LDAP	Dostępność: tylko Samsung SDK
Blokada tworzenia konta Samsung	Dostępność: tylko Samsung SDK
Blokada aparatu	Zablokuj możliwość korzystania z aparatu. Dostępność: Android BYOD i WPC
Wyłącz możliwość kopiowania-wklejania w profilu	Dostępność: Android BYOD i WPC
Wyłącz możliwość kontrolowania aplikacji	Blokuje następujące akcje: odinstalowywanie i wyłączanie aplikacji, czyszczenie pamięci podręcznej i danych aplikacji, wymuszanie zatrzymywania aplikacji i czyszczenie ustawień domyślnych aplikacji Dostępność: Android BYOD i WPC
Wyłącz możliwość użycia tej samej blokady dla urządzenia oraz profilu służbowego	Blokuje możliwość użycia jednego kodu blokady dla urządzenia i profilu służbowego. Dostępność: Android BYOD i WPC
Zezwalaj na przenoszenie aplikacji do profilu do pracy	Dostępność: tylko Samsung SDK
Blokada NFC	Dostępność: tylko Samsung SDK
Nie zezwalaj na przesyłanie danych za pomocą NFC	Dostępność: Android BYOD i WPC

Zezwalaj na przenoszenie plików z urządzenia do profilu do pracy	Dostępność: tylko Samsung SDK
Zezwalaj na przenoszenie plików z profilu do pracy do urządzenia	Dostępność: tylko Samsung SDK
Blokada zmiany udostępniania kalendarza do trybu osobistego	Dostępność: tylko Samsung SDK
Blokada zmiany udostępniania kalendarza do profilu do pracy	Dostępność: tylko Samsung SDK
Aktywacja interfejsu Bluetooth	Dostępność: tylko Samsung SDK
Włącz udostępnianie plików przez Bluetooth w profilu do pracy	Dostępność: Android BYOD i WPC
Blokada udostępniania przez Share Via List	Dostępność: tylko Samsung SDK
Zablokuj konfigurację poświadczeń przez użytkowników w zarządzanym magazynie kluczy	Dostępność: Android BYOD i WPC
Maksymalny czas, przez jaki profil do pracy może być wyłączony	Po przekroczeniu czasu aplikacje osobiste są blokowane. Możliwe opcje: Niepełnosprawni lub 3-14 dni Dostępność: Android WPC 11+
Włącz możliwość przywrócenia kopii zapasowej z konta Google	Przywracanie danych z kont prywatnych jest domyślnie wyłączone, zaznacz tę opcję, aby ją włączyć Dostępność: Android BYOD i WPC
Wyłącz możliwość włączania lokalizacji w ustawieniach	Blokuje możliwość zmiany ustawień lokalizacji Dostępność: Android BYOD i WPC
Wyłącz możliwość udostępniania lokalizacji	Dostępność: Android BYOD i WPC
Wyłącz przechwytywanie treści	Dostępność: Android BYOD i WPC
Wyłącz sugestie dotyczące treści	Dostępność: Android BYOD i WPC
Upewnienia aplikacji w profilu do pracy	

Globalny dostęp aplikacji	Ustawienie odpowiedzialne za zachowanie aplikacji, które proszą o konkretne uprawnienia podczas pracy. Możesz ustawić trzy wartości: • Zarządzane przez użytkownika - wartość domyślna, użytkownik zostanie poproszony o przyznanie aplikacji dostępu do funkcji, które wymagają specjalnego pozwolenia. Użytkownik będzie również mógł zmieniać uprawnienia dla aplikacji. • Zezwalaj - aplikacje, które proszą o uprawnienia, będą je automatycznie otrzymywać, a użytkownik nie będzie mógł ich zmienić. • Odmów - aplikacje, które proszą o uprawnienia, będą automatycznie odrzucane, a użytkownik nie będzie mógł ich zmienić.
Samsung KSP dla profilu do pracy	
Włącz Samsung Knox Service Plugin	Knox Service Plugin (KSP) to rozwiązanie umożliwiające konfigurowanie polityk i zarządzanie urządzeniami mobilnymi obsługującymi platformę Samsung Knox dla przedsiębiorstw (KPE). Procedura konfiguracji KSP opisana jest w osobnym dokumencie dostępnym tutaj. Listę wszystkich dostępnych parametrów można znaleźć tutaj: https://docs.samsungknox.com/admin/knox-service-plugin/release-notes.htm

3.6 Włączone aplikacje i widgety

W tej sekcji Administrator może udostępnić aplikacje systemowe Google w profilu służbowym, aby były automatycznie dostępne dla użytkowników po aktywacji profilu. Udostępnione aplikacje na urządzeniu mogą się różnić, ponieważ niektóre wersje Androida (szczególnie wersje markowe) mogą nie obejmować wszystkich wymienionych aplikacji systemowych. Administrator może zmienić listę włączonych aplikacji i ukryć je zgodnie z potrzebami. Domyślne aplikacje, które są zawsze widoczne po aktywacji profilu, to FAMOC Base Agent i zarządzany sklep Google.

		Dostępność	
		Android	Samsung SDK
Google Maps	☒	✓	✗
Kalendarz	☒	✓	✗
Aparat	☒	✓	✗
Galeria	☒	✓	✗
Telefon	☒	✓	✗
Wiadomości	☐	✓	✗
Google Drive	☒	✓	✗
Kontakty	☒	✓	✗
Pobrane	☒	✓	✗

Rysunek 30 Menu dostępności aplikacji w profilu służbowym

W sekcji widżetów możesz włączyć widżet aplikacji firmowych - zainstalowanych w profilu do pracy - do używania na ekranie głównym urządzenia (muszą zostać dodane ręcznie przez użytkownika końcowego). Nazwę pakietu należy dodać do listy. Widżety aplikacji będą teraz dostępne do dodania na ekranie głównym.

3.7 Zaawansowane

W zakładce ustawień zaawansowanych można ustawić następujące parametry:

Atrybut	Opis
Zaawansowane ustawienia polityk	
Ilość zapamiętanych sesji Monitora urządzenia	Określa, ile sesji Monitora urządzenia ma być przechowywanych przez FAMOC (1-10) Wartość domyślna: 5
Ilość archiwalnych sesji Monitora urządzenia:	Określa, ile sesji Monitora urządzenia ma być przechowywanych w logach (10-150) Default value: 20
Dane raportowane w sesji Monitora urządzenia	Wybierz, które dane będą raportowane przez monitor użytkownika. Wartość domyślna: Wszystkie (możliwe wybory: parametry podstawowe; aplikacje; Bluetooth; dyski; punkty dostępu; certyfikaty; administratorzy urządzeń; konta na urządzeniu; aktualizacje oprogramowania; karty SIM)
Interwał synchronizacji czasu	Ustawia, jak często zegar systemowy urządzenia S60 jest zsynchronizowany z serwerem Network Time Protocol Wartość domyślna: Wyłączony
Informowanie o zmianie karty SIM (np. podczas kradzieży telefonu)	Tak/Nie Wartość domyślna: Nie
Limit urządzeń na użytkownika	Liczba urządzeń, które użytkownik może dodać za pomocą strony startowej, gdy ustawiana jest opcja autoryzacji użytkownika. Jeśli limit zostanie przekroczony, użytkownik nie może dodawać żadnego innego urządzenia do systemu za pomocą strony startowej.
Nazwa organizacji wyświetlana na urządzeniu	Wprowadzony tekst zostanie wyświetlony na ekranie blokady urządzenia.

Pokaż drugą linię w nagłówku FAMOC Base Agent	Tak lub nie
Wartość drugiej linii w nagłówku FAMOC Base Agent	Pobierane z wybranego pola

Ciągłe raportowanie i ostrzeganie o parametrach

W tej sekcji możesz zdefiniować, które parametry baterii będą raportowane w czasie rzeczywistym. Możesz włączyć raportowanie ciągłe lub szczytowe. Jeśli stan baterii przekroczy określony próg lub status, w konsoli zarządzania FAMOC pojawi się alert.

Dostępne parametry są wymienione poniżej:

- Stan baterii - gdy raportowana wartość różni się od podanej (np. określono: dobry, zaraportowane: przegrzanie)
- Poziom naładowania baterii - gdy raportowana wartość jest niższa niż określona 10%-50%
- Temperatura akumulatora - gdy raportowana wartość jest wyższa niż określone 20-100 stopni Celsjusza
- Napięcie akumulatora - gdy raportowana wartość jest wyższa niż podana 2V-10V
- Stan ładowarki - gdy raportowany stan różni się od podanego (np. określony: Podłączony, raportowany: Brak połączenia)
- Niski poziom baterii - gdy zgłaszana wartość jest równa podanej
- Pamięć RAM Wolna - gdy raportowana wartość jest niższa niż określona (10-50%)
- Siła sygnału - gdy raportowana wartość jest niższa niż określona (np. określona: -80 dBm, raportowana: -107 dBm)

Szczegóły urządzenia w agencji bazowym

Administrator może dodać niestandardowe pola, które będą wyświetlane na karcie **Informacje o urządzeniu**.

Lista pól		Dodaj pole
Model	▼	×
Platforma	▼	×
IMEI	▼	×
WLAN MAC	▼	×
Użytkownik	▼	×
Status trybu Device Owner	▼	×
Status KNOX	▼	×
Status profilu do pracy	▼	×

Rysunek 31 Pola szczegółów urządzenia

Ustawienia kopii zapasowej

W tej sekcji możliwe jest ustawienie synchronizacji wszystkich kontaktów lub synchronizację danych tylko w grupach, których członkiem jest użytkownik. W przypadku tej drugiej opcji administrator może określić dodatkowe grupy, z których będą zsynchronizowane kontakty. Aby dodać grupy użytkowników do synchronizacji danych kontaktowych, użyj przycisku Wybierz. Możesz także ustawić interwał synchronizacji kontaktów codziennie, co tydzień lub co miesiąc.

Ustawienia kopii zapasowej

Ustawienia synchronizacji kopii zapasowej:

Interwał kopii zapasowej *: Raz dziennie ▼

Synchronizacja kontaktów biznesowych:

Podstawowy typ synchronizacji: Żadne kontakty ▼

Interwał synchronizacji kontaktów biznesowych: Wyłączona ▼

Synchronizacja kontaktów z dodatkowych grup Wybierz

Nazwa grupy	Liczba użytkowników	Przypisani użytkownicy	
Harvey Group	1	Harvey Specter	×
Mike Group	3	Mike Ross, Mike Bird, ff.michalk@outlook.com	×

Rysunek 32 Ustawienia synchronizacji kontaktów

Polityka monitora użycia

Ta sekcja umożliwia ustawienie monitorowania użytkownika, w tym:

- Raportowanie przesyłu danych za pomocą WIFI
- Raportowanie przesyłu danych za pomocą GPRS
- Zgłaszanie treści SMS
- Raportowanie typu połączenia

Zaznaczenie pola wyboru **Włącz monitor użycia** aktywuje polityki użytkownika. W takim przypadku na urządzeniu zostanie zainstalowany Monitor użycia z uwzględnieniem adekwatnych polityk.

Atrybut	Opis
Ustawienia polityki monitora użycia	
Włącz monitor użycia	Jeśli ta opcja jest zaznaczona, Monitor użycia zostanie zainstalowany wraz z polityką. Wartość domyślna: niezaznaczona.
Raportuj dane po restarcie urządzenia	Jeśli zostanie ustawiony, Monitor użycia będzie zbierać i wysyłać dane po ponownym uruchomieniu urządzenia.
Raportuj użycie danych po WIFI co:	Interwał w raportowaniu danych WIFI (Nie zgłaszaj/1 dzień/3 dni/1 tydzień/2 tygodnie/1 miesiąc/3 miesiące). Wartość domyślna: 1 miesiąc.
Raportuj użycie danych po GPRS co:	Interwał w raportowaniu danych GPRS (Nie zgłaszaj/1 dzień/3 dni/1 tydzień/2 tygodnie/1 miesiąc/3 miesiące). Wartość domyślna: 1 miesiąc.
Raportuj treść SMS	Jeśli zostanie ustawione, treść SMS będzie raportowana. Wartość domyślna: niezaznaczona.
Raportuj stan urządzenia	Jeśli jest ustawione, raportuje stan urządzenia. Wartość domyślna: niezaznaczona.
Raportuj czas odblokowania/zablokowania ekranu	Zaznacz, aby zebrać informacje o tym, kiedy ekran został odblokowany.
Raportuj użycie aplikacji⁶	Jeśli jest ustawione, raportuje użycie aplikacji. Wartość domyślna: niezaznaczona.
Raportuj historię przeglądarki	Jeśli jest ustawione, raportuje historię przeglądarki. Wartość domyślna: niezaznaczona.
Raportuj rozszerzone parametry co:	Interwał raportowania stanu urządzenia, użycia aplikacji i historii przeglądarki (Nie zgłaszaj/15 minut/30 minut/1 godzina/6 godzin/1 dzień/3 dni/1 tydzień/2 tygodnie/1 miesiąc) Wartość domyślna: 1 dzień.
Pozwalaj użytkownikowi wybrać typ rozmowy	Jeśli wybrano Zezwalaj , przy wykonywaniu połączenia użytkownik zostanie poproszony o wybranie typu. Lista typów połączeń może być zmieniana. Domyślnie dostępne są dwa

⁶ W przypadku systemu Android 6.0 lub nowszego raportowanie użycia aplikacji wymaga włączenia na urządzeniu usługi Application Monitor Service.

	typy: prywatne/firmowe. Wartość domyślna: nie zezwalaj.
--	--

Ustawienia polityki monitora użycia

Włącz monitor użycia: ☒

Raportuj dane po restarcie urządzenia: ☒

Ustawienia danych pakietowych

Raportuj użycie danych po WIFI co: 1 dzień

Raportuj użycie danych po GPRS co: 1 dzień

Ustawienia wiadomości

Raportuj treść SMS: ☒

Ustawienia rozszerzonego raportowania

Raportuj stan urządzenia: ☒

Raportuj użycie aplikacji: ☒

Raportuj historię przeglądarki: ☒

Raportuj rozszerzone parametry co: 1 dzień

Ustawienia raportowania rozmowy głosowej

Pozwalaj użytkownikowi wybrać typ rozmowy: Nie pozwalaj

Rysunek 33 Ustawienia polityki monitora użycia

4. Polityki COSU

Polityki COSU pozwalają na szybką konfigurację urządzeń dedykowanych. Urządzenia z przypisaną tą polityką będą działać w trybie kiosk, co oznacza że dostępne na nich będą jedynie dozwolone aplikacja/aplikacje.

4.1 Ustawienia podstawowe

Aby dodać ogólny szablon polityk, podaj nazwę i ustaw priorytet.

Atrybut	Opis
Ustawienia podstawowe	
Nazwa szablonu	Wprowadź nazwę polityki (maks. 100 znaków)
Ustaw priorytet	Określ pozycję na liście szablonów
Przeinstaluj Base Agenta automatycznie	Po pojawieniu się w systemie nowej wersji programu Base Agent zostanie ona automatycznie ponownie zainstalowana na urządzeniach (polityka zostanie ustawiona jako nieaktualna). Wartość domyślna: niezaznaczone.

Odinstaluj niezgodne elementy polityki automatycznie	Jeśli ta opcja jest zaznaczona, niepasujące elementy z bieżącej polityki zostaną odinstalowane, jeśli urządzenie zostanie przypisane do innej polityki. Wartość domyślna: niezaznaczone.
Oznacz urządzenie jako wyczyszczone przy wykrytym odinstalowaniu Agenta Bazowego	Jeśli ta opcja jest zaznaczona, urządzenie zostanie oznaczone w konsoli FAMOC jako wyczyszczone w przypadku odinstalowania Agenta Bazowego. Wartość domyślna: niezaznaczone.
Włącz usługi zdalnego pulpitu	Jeśli ta opcja jest zaznaczona, Zdalny dostęp zostanie zainstalowany wraz z polityką. Wartość domyślna: niezaznaczone.
Włącz usługi lokalizacyjne	Jeśli ta opcja jest zaznaczona, Monitor lokalizacji zostanie zainstalowany wraz z polityką. Wartość domyślna: niezaznaczone.
Raportuj dodatkowe informacje o aplikacjach (rozmiar aplikacji, rozmiar pamięci podręcznej, rozmiar danych)	
Raportowane aplikacje	

▼ Ustawienia podstawowe

Nazwa szablonu:

Ustaw priorytet:

Przeinstaluj Base Agenta automatycznie: ☐

Odinstaluj niezgodne elementy polityki automatycznie: ☐

Włącz Samsung Premium API: ☒

Licencja premium: - - - - - +

Włącz atestację Samsung: ☐

Włącz atestację Safetynet: ☐

Oznacz urządzenie jako wyczyszczone przy wykrytym odinstalowaniu Agenta Bazowego: ☐

Włącz usługi zdalnego pulpitu: ☐

Włącz usługi lokalizacyjne: ☐

Wymuszaj włączenie usługi monitorowania aplikacji: ☐

Ignoruj optymalizację zużycia baterii dla Monitora lokalizacji i Monitora użycia *: ☐

Rysunek 34 Zakładka ustawień podstawowych

4.1.1. Ustawienia harmonogramów

Poniżej znajduje się lista parametrów ustawień harmonogramów polityk.

Atrybut	Opis
Ustawienia harmonogramów	
Interwał synchronizacji w szczycie	Interwał połączenia z serwerem Base Agent: 5 min./15 min./30 min./1 g./4 g./12 g./Raz dziennie/Raz w tygodniu/Raz w miesiącu Wartość domyślna: raz dziennie
Dni szczytu	Dni tygodnia, w trakcie których Agent Bazowy raportuje do serwera FAMOC Wartość domyślna: od poniedziałku do piątku
Początek szczytu	O której godzinie w dniach szczytu powinien zacząć raportowanie agent podstawowy Wartość domyślna: 8:00
Koniec szczytu	O której godzinie w dniach szczytu powinien zakończyć raportowanie agent podstawowy Wartość domyślna: 16:00
Interwał sesji Monitora Urządzenia	Ustawia interwał sesji Monitora Urządzenia: Wyłączony/Co godzinę, 4 razy dziennie/Codziennie/Raz w tygodniu/Raz w miesiącu Wartość domyślna: Codziennie
Informowanie o nieaktywności urządzenia	Ostrzeganie o bezczynności agenta bazowego po: 1-5 dniach/tygodniu/miesiącu/3 miesiącach. Jeśli agent bazowy nie połączy się z serwerem w tym okresie, FAMOC wygeneruje alert z trzema możliwymi opcjami reakcji: • Usuń urządzenie z FAMOC • Zainstaluj ponownie program Base Agent • Oznacz urządzenie jako skradzione Wartość domyślna: po tygodniu
Wyczyść urządzenie przy przekroczonej nieaktywności	Jeśli ta opcja jest zaznaczona, a agent bazowy nie zgłasza się do serwera w określonym czasie, oprócz wygenerowanego alertu urządzenie zostanie wyczyszczone.
Oznacz urządzenie jako wyczyszczone przy przekroczonej nieaktywności	W przypadku przekroczenia czasu zgłoszenia się urządzenia do serwera, zostanie ono oznaczone w konsoli FAMOC jako wyczyszczone.

Ustawienia harmonogramów

Interwał synchronizacji w szczycie: Raz dziennie

Dni szczytu: ☒ Poniedziałek ☒ Wtorek ☒ Środa ☒ Czwartek ☒ Piątek ☐ Sobota ☐ Niedziela

Początek szczytu: 08:00

Koniec szczytu: 16:00

Interwał sesji Monitora urządzenia: Dzień

Informowanie o nieaktywności urządzenia: Po tygodniu

Wyczyść urządzenie przy przekroczonej nieaktywności: ☐

Oznacz urządzenie jako wyczyszczone przy przekroczonej nieaktywności: ☐

Rysunek 35 Ogólne ustawienia polityk

4.2 Przypisane grupy

Każda polityka przypisana jest do określonych grup użytkowników lub grup urządzeń, dlatego każde urządzenie otrzymuje ustawienia polityk wstępnie zdefiniowane do przypisanej grupy. Urządzenia nienależące do żadnej grupy oraz grupy, które nie są przypisane do żadnej polityki, otrzymują politykę o najniższym priorytecie (polityka znajdująca się na dole listy). Urządzenia przypisane do kilku grup otrzymują politykę o wyższym priorytecie.

W zakładce **Grupy** administrator może przydzielać grupy do polityk. Aby wybrać grupę, kliknij przycisk **Dodaj grupę urządzeń** lub przycisk **Dodaj grupę użytkowników**. Zostanie wyświetlone okno z listą grup.

Grupy użytkowników

Dodaj grupę użytkowników

Nazwa grupy	Liczba użytkowników	Przypisani użytkownicy

Zaznacz pola wyboru obok odpowiednich grup i kliknij Wybierz. Grupy zostaną teraz przypisane do polityki.

4.3 Elementy polityk

Oprócz ogólnych ustawień istnieje możliwość dodania konfiguracji i aplikacji do polityki.

Aby dodać konfigurację do polityki, kliknij przycisk **Wybierz konfigurację**. Pojawi się okno z listą konfiguracji.

Konfiguracja może być ustawiona dla:

- Szczytu – konfiguracja zostanie zastosowana w okresie szczytu
- Poza szczytem – konfiguracja zostanie zastosowana poza okresem szczytu
- Zawsze – konfiguracja będzie zawsze stosowana

Za każdym razem, gdy urządzenie łączy się z serwerem, sprawdza, czy zastosowana jest odpowiednia polityka, a jeśli potrzebna jest zmiana (np. zakończył się okres szczytu, a aktualnie stosowana konfiguracja dotyczy tylko tego okresu), stara konfiguracja jest usuwana,

a zastosowana jest odpowiednia. Polityki oparte na czasie mogą być stosowane tylko na urządzeniach z systemem iOS.

Aby dodać aplikację, kliknij przycisk **Wybierz aplikację**. Pojawi się okno z listą aplikacji. Wybrane aplikacje zostaną zainstalowane podczas przypisywania polityk do urządzenia. Po zmianie polityk przypisanych do urządzenia zastosowane zostaną nowe polityki i zainstalowana nowa lista aplikacji. Podczas wyboru aplikacji, można określić liczbę powtórzeń instalacji (w przypadku anulowania instalacji przez użytkownika, FAMOC ponowi operację). Możliwe opcje:

- Instalacja obowiązkowa (opcja domyślna) - jeśli instalacja zostanie anulowana, będzie powtarzana co dzień.
- Jedna próba instalacji - jeśli instalacja zostanie anulowana, nie będzie ponawiana.
- Kilka prób instalacji - instalacja będzie ponawiana określoną liczbę razy.

Elementy polityki można ustawić w niestandardowej kolejności instalacji, używając strzałek w dół/w górę w kolumnie **Kolejność**.

Domyślnie każdy element jest instalowany w sekwencji (następny element rozpoczyna się po pomyślnym zainstalowaniu poprzedniego). Można jednak oznaczyć element jako niezależny (kolumna **Niezależny**), co oznacza, że kolejna akcja rozpoczyna się niezależnie od poprzedniej, nie czekając na raport z powodzeniem.

Zaznacz opcję **Ignoruj błąd**, aby wykonać następną akcję, jeśli poprzednia zakończyła się niepowodzeniem.

Elementy polityki					
Nazwa elementu		Akcja	Ignoruj błąd	Niezależny	Kolejność
Require 4 chars lock code on Android	Polityka szczytu:	Zawsze ▾	☐	☐	↓ ×
Tapeta FF 1080p	Polityka szczytu:	Zawsze ▾	☐	☐	↑ ×

Rysunek 11 Elementy polityki

4.4 Ustawienia trybu COSU

Tutaj możesz skonfigurować ustawienia trybu kiosku. Przede wszystkim wybierz, czy chcesz używać programu uruchamiającego FAMOC tylko z aplikacjami z białej listy lub pojedynczą aplikacją. Niezależnie od twojego wyboru, będziesz musiał podać nazwę pakietu lub nazwy aplikacji na białej liście.

Tryb blokady

FAMOC Launcher z listą dozwolonych aplikacji ▾

▾

Lista aplikacji dozwolonych w FAMOC Launcher

Lista dozwolonych aplikacji w FAMOC Launcher

Dodaj aplikację

Nazwa paczki	
com.android.chrome	×
com.android.email	×

Pozostałe ustawienia wymieniono poniżej:

Parametr	Wartość
Ustawienia COSU	
Tryb blokady	- FAMOC Launcher z listą dozwolonych aplikacji - Pojedyncza aplikacja
Ustawienia dla FAMOC Launcher	
Tapeta	Możliwość wgrania tapety
Pokaż pasek stanu	Możliwe ustawienia: Tak/Nie
Pokaż niestandardowy pasek ustawień	Jeśli włączone, zostanie wyświetlony pasek ustawień niestandardowych. Dodatkowe ustawienia: - Pozycja - położenie paska na ekranie - Motyw - jasny lub ciemny - Pole niestandardowe - Możliwość wyświetlenia dodatkowych informacji pobranych z wybranego pola niestandardowego. - Pokaż ikonę Bluetooth - Pokaż ikonę WIFI - Pokaż ikonę latarki - Pokaż ikonę restartu
Lista dozwolonych aplikacji	Tutaj możesz podać listę dozwolonych aplikacji w FAMOC Launcher
Skróty	Tutaj możesz podać listę skrótów do aplikacji i klipów internetowych w FAMOC Launcher
Ustawienia dla pojedynczej aplikacji	
Nazwa pakietu aplikacji	Należy wprowadzić nazwę pakietu aplikacji np com.android.chrome
Ustawienia COSU	
Zmiana głośności	Możliwe opcje: włączona/wyłączona.
Długie naciśnięcie przycisku zasilania	Możliwe opcje: włączone/wyłączone. Dostępne dla urządzeń z Android 9.0 lub nowszym.
Ochrona klawiatury	Możliwe opcje: włączona/wyłączona. Dostępne dla urządzeń z Android 9.0 lub nowszym.

Przycisk ekranu głównego	Możliwe opcje: włączony/wyłączony. Dostępne dla urządzeń z Android 9.0 lub nowszym.
Ostatnie aplikacje	Możliwe opcje: włączony/wyłączony. Dostępne dla urządzeń z Android 9.0 lub nowszym.
Powiadomienia	Możliwe opcje: włączony/wyłączony. Dostępne dla urządzeń z Android 9.0 lub nowszym.
Informacje o systemie na pasku stanu	Możliwe opcje: włączone/wyłączone. Dostępne dla urządzeń z Android 9.0 lub nowszym.
Domyślne aplikacje do otwierania dokumentów	Możliwość zdefiniowania domyślnej aplikacji do otwierania dokumentów (np. .pdf, .xls). Aby to zrobić rozwiń listę i kliknij Dodaj domyślną aplikację. Następnie wybierz typ pliku z rozwijanej listy i wprowadź odpowiednie parametry w poniższych polach. Dla najpopularniejszych aplikacji możliwe jest zastosowanie domyślnych schematów ustawień.

4.5 Opcje bezpieczeństwa

W ramach opcji bezpieczeństwa dostępne są następujące ustawienia:

1. Polityka czyszczenia danych
2. Polityka sieci
3. Polityka lokalizacji
4. Polityka aktualizacji
5. Polityka sprzętowa
6. Polityka szyfrowania pamięci
7. Polityka instalatora
8. Ograniczenia aplikacji
9. Polityka aplikacji
10. Samsung KSP

4.5.1 Polityka czyszczenia danych

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka czyszczenia danych**.

Atrybut	Opis
Polityka czyszczenia danych	
Czyszczenie pamięci telefonu po wykryciu zmiany karty SIM	Jeśli ustawione, czyszczenie zostanie wykonane po wykryciu zmiany karty SIM. Dostępność: urządzenia z systemem Android
Reaguj również na brak karty	Jeśli ustawione, czyszczenie zostanie wykonane, gdy karta SIM nie zostanie wykryta. Opcja dostępna po ustawieniu pierwszej opcji (Czyszczenie danych przy zmianie karty SIM).

	OSTRZEŻENIE! Po zastosowaniu tej konfiguracji użytkownicy nie będą mogli korzystać z trybu samolotowego Androida, ponieważ spowoduje to wymazanie urządzenia. Dostępność: urządzenia z systemem Android
Wyczyść również kartę pamięci	Jeśli ustawione, po wykryciu zmiany karty SIM dodatkowo zostanie wyczyszczona karta pamięci. Opcja dostępna po ustawieniu pierwszej opcji (Czyszczenie danych przy zmianie karty SIM). Dostępność: urządzenia z systemem Android
Czyszczenie urządzenia po wykryciu rootowania	Jeśli ustawione, urządzenie zostanie wyczyszczone po wykryciu rootowania. Dostępność: urządzenia z systemem Android.
Blokada przywracania ustawień fabrycznych	Jeśli włączona, uniemożliwia wykonanie resetu do ustawień fabrycznych. Dostępność: Device Owner, Android Samsung 4.x z Enterprise SDK 2.0, Android LG z Enterprise SDK from 1.0 , Windows Phone 8.1/10
Ochrona przywracania do ustawień fabrycznych (FRP)⁷	Factory Reset Protection to rozwiązanie, które umożliwia uruchomienie urządzenia po przywróceniu ustawień fabrycznych jedynie kontem Google, którym wcześniej zalogowano się na urządzeniu. Dostępne możliwości konfiguracji tego ustawienia: • wyłączona (opcja nie będzie dostępna) • odblokuj urządzenie aktywnym kontem (urządzenie można odblokować poprzednio używanym kontem) • odblokuj urządzenie za pomocą konta z listy (urządzenie można odblokować kontem z wprowadzonej listy - należy podać id użytkownika) • zdejmij blokadę FRP po wyczyszczeniu urządzenia (wyłącza blokadę po wyczyszczeniu urządzenia) Dostępność: Device Owner

4.5.2 Polityka sieci

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka sieci**.

Atrybut	Opis
---------	------

⁷ Lista kont do odblokowania musi zawierać prawidłowe identyfikatory użytkownika Google. Można je uzyskać z Google API, korzystając z linku poniżej:

<https://developers.google.com/people/api/rest/v1/people/get>

Wykonując wywołanie interfejsu API i logując się przy użyciu prawidłowego konta Google, odpowiedź zwraca „id” użytkownika.

Polityka sieci	
Blokada interfejsu Wi-Fi	Jeśli włączona na urządzeniu niemożliwe będzie korzystanie z Wi-Fi. Dostępność: urządzenia z systemem Android i Windows Phone 8.1 / 10
Blokada ręcznej konfiguracji Wi-Fi	Jeśli włączona, nie będzie możliwości ręcznej konfiguracji Wi-Fi. Dostępność: Tryb Device Owner, urządzenia iOS w trybie nadzorowanym, Windows Phone 8.1 / 10
Utrzymuj Wi-Fi włączone w trybie uśpienia	Jeśli włączona połączenie z siecią bezprzewodową będzie podtrzymywane również w trybie uśpienia. Dostępność: Tryb Device Owner
Blokada interfejsu Bluetooth	Jeśli włączona, na urządzeniu nie może być używana komunikacja Bluetooth. Dostępność: Android, Windows Phone 8.1 / 10, iOS 11.3 i nowsze w trybie nadzorowanym
Blokada danych pakietowych	Możliwe wybory: • Nie blokuj • Włącz i zablokuj możliwość wyłączenia • Wyłącz i zablokuj możliwość włączenia Dostępność: Android Wartość domyślna: Nie blokuj.
Blokada danych pakietowych w roamingu	Możliwe wybory: • Nie blokuj • Wyłącz i zablokuj możliwość włączenia Dostępność: Android, Tryb Device Owner i urządzenia Windows Phone 8.1 / 10 Wartość domyślna: Nie blokuj.
Blokada udostępniania internetu przez WiFi	Jeśli włączona, udostępniania internetu przez WiFi zostanie wyłączone. Dostępność: Android Samsung z Enterprise SDK od 2.0 i Tryb Device Owner
Blokada udostępniania internetu przez USB	Jeśli włączona, udostępnianie internetu przez USB jest wyłączone. Dostępność: Android Samsung z Enterprise SDK od 3.0, Tryb Device Owner oraz Windows Phone 8.1 / 10
Blokada przychodzących wiadomości MMS	Jeśli włączona przychodzące wiadomości MMS nie będą dostarczane. Dostępność: Android Samsung z Enterprise SDK from 3.0

Wyłącz możliwość resetowania ustawień sieci	Blokuje możliwość korzystania z opcji "Resetuj ustawienia sieciowe". Dostępność: tryb Device Owner
Wyłącz ustawienia VPN	Blokuje możliwość modyfikowania ustawień VPN Dostępność: tryb Device Owner
Blokuj ustawienia prywatnych DNS	Jeśli jest ustawiony, użytkownik nie może ustawić prywatnego DNS ani wyłączyć DNS przez TLS na urządzeniu. Dostępność: Urządzenia w trybie Device Owner z systemem Android 10.0+
Zablokuj przychodzące rozmowy	Umożliwia blokowanie połączeń przychodzących. Dostępne opcje: • Nie blokuj • Wszystkie • Wg wzoru (Wzór blokowanych numerów może zawierać np. numery rozpoczynające się od 0700) Dostępność: Samsung SDK
Zablokuj przychodzące wiadomości SMS	Umożliwia blokowanie przychodzących wiadomości tekstowych. Dostępne opcje: • Nie blokuj • Wszystkie • Wg wzoru (Wzór blokowanych numerów może zawierać np. numery rozpoczynające się od 0700) Dostępność: Samsung SDK
Monitoruj listę zarządzanych konfiguracji Wi-Fi	Monitoruje stan zarządzanych sieci i wyzwala alert w przypadku ich usunięcia (zapomnienia na urządzeniu).

4.5.3 Polityka lokalizacji

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka lokalizacji**.

Atrybut	Opis
Polityka lokalizacji	
Blokada lokalizacji	Pozwala przyznać agentowi FAMOC dostęp do lokalizacji i blokuje możliwość cofnięcia tych uprawnień. Możliwe opcje: • Nie blokuj • Włącz lokację • Włącz lokalizację i zablokuj możliwość wyłączenia • Wyłącz lokalizację • Wyłącz lokalizację i zablokuj możliwość włączenia

	Dostępność: Android, Device Owner Wartość domyślna: Nie blokuj
--	---

4.5.4 Polityka aktualizacji

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka aktualizacji**.

Atrybut	Opis
Polityka aktualizacji	
Kontroluj wersję systemu (Samsung E-FOTA)	Jeśli włączona, umożliwia obsługę E-FOTA. Dostępność: Android Samsung 7.x z Knox 2.7.1+
Polityka aktualizacji OTA	Możliwość zdefiniowania polityki aktualizacji OTA. Dostępne opcje to: • Brak polityki • Automatyczna • Według harmonogramu • Wstrzymana Dostępność: Device Owner (blokuje aktualizację systemu na 30 dni), Android Samsung z Enterprise SDK 3.0

4.5.5. Polityka sprzętowa

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka sprzętowa**.

Atrybut	Opis
Polityki sprzętowe	
Blokada aparatu	Jeśli włączona, wyłącza możliwość korzystania z aparatu. Dostępność: tryb Device Owner, Android 4.x, Android Samsung 2.3 – 4.x oraz Windows Phone 8.1/10, iOS
Blokada trybu odtwarzacza multimedialnych przez USB	Jeśli włączona, a urządzenie jest podłączone do komputera przez USB, nie można użyć do w trybie odtwarzacza multimedialnych. Dostępność: Android Samsung 4.x z Enterprise SDK 3.0, Android Sony z Enterprise SDK od 5.0
Blokada opcji programisty	Uniemożliwia włączenie trybu programowania. Dostępność: tryb Device Owner, Android Samsung z Enterprise SDK 5.0
Blokada menadżera zadań	Jeśli włączona, uniemożliwia korzystanie z menadżera zadań.

	Dostępność: Android Samsung z Enterprise SDK 3.0
Blokada NFC	Uniemożliwia korzystanie z NFC. Dostępność: Windows Phone 8.1/10, Android Samsung z Enterprise SDK od 2.0
Nie zezwalaj na przesyłanie danych za pomocą NFC	Jeśli ustawiona, użytkownik nie może używać NFC do przesyłania danych z aplikacji. Dostępność: tryb Device Owner
Blokada kart pamięci	Uniemożliwia korzystanie z gniazda kart pamięci. Dostępność: Device Owner, Android Samsung with Enterprise SDK from 2.0, Windows Phone 8.1/10
Blokada przechwytywania obrazu	Jeśli włączona, uniemożliwia wykonywanie zrzutów ekranu Dostępność: Device Owner, Windows Phone 8.1/10, Android Samsung z Enterprise SDK od 2.0 oraz urządzenia z iOS
Blokada trybu przeglądania plików USB	Jeśli włączona, nie będzie możliwości przeglądania plików przez połączenie USB. Dostępność: Device Owner, Windows Phone 8.1/10
Blokada wielu okien	Jeśli włączona, tryb wielu okien nie będzie dostępny na urządzeniu Dostępność: Android Samsung with Enterprise SDK from 4.0
Blokada trybu awaryjnego	Jeśli opcja zostanie ustawiona, na urządzeniu nie będzie dostępny tryb awaryjny. Dostępność: Device Owner, Android Samsung z Enterprise SDK od 4.0
Blokada trybu samolotowego	Jeśli opcja zostanie ustawiona, na urządzeniu nie będzie dostępny tryb samolotowy. Dostępność: Android Samsung z Enterprise SDK od 5.0
Zablokuj konfigurację poświadczeń przez użytkowników w zarządzanym magazynie kluczy	Jeśli ustawione, użytkownik nie będzie miał dostępu do niektórych opcji przechowywania poświadczeń, takich jak: Wyświetl certyfikaty użytkownika, Zainstaluj certyfikaty z pamięci urządzenia, Usuń certyfikaty Dostępność: Device Owner

4.5.6 Polityka szyfrowania pamięci

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka szyfrowania**.

Atrybut	Opis
---------	------

Polityki szyfrowania	
Szyfrowanie pamięci wewnętrznej	Jeśli opcja zostanie ustawiona, wymagane będzie szyfrowanie. Dostępność: Android 4.x oraz Android Samsung z Enterprise SDK 2.0/3.0, iOS oraz Windows Phone 8.1/10

4.5.7 Polityka instalatora

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka instalatora**.

Atrybut	Opis
Polityki instalacji	
Blokada instalacji aplikacji	Jeśli włączona, nie będzie możliwości instalowania aplikacji na urządzeniu. Dostępność: Android, Apple, Windows Phone 8.1 / 10, urządzenia w trybie Device Owner
Zezwól na debugowanie USB	Jeśli ustawione, zezwala na uruchomienie na urządzeniu trybu debugowania USB. Dostępne dla trybu Device Owner, Android Samsung z Enterprise SDK 3.0, dla Android Sony z Enterprise SDK od 5.0 oraz Windows Phone 8.1/10. USB debugging is blocked by default.
Blokada nieznanych źródeł	Uniemożliwia zmianę ustawień instalacji z nieznanych źródeł. Dostępność: tryb Device Owner, Android Samsung z Enterprise SDK 2.0 oraz Windows 10 Mobile
Wyłącz możliwość modyfikowania kont	Jeśli włączona, możliwość dodania, edycji lub usunięcia konta zostanie zablokowana Dostępność: tryb Device Owner oraz urządzenia iOS w trybie nadzorowania
Wyłącz możliwość kontrolowania aplikacji	Jeśli włączona, użytkownicy nie będą mogli modyfikować aplikacji (odinstalować, zatrzymać działanie, wyczyścić dane aplikacji). Dostępność: Android Device Owner

4.5.8 Ograniczenia aplikacji

Poniżej znajduje się lista ustawień dostępnych w zakładce **Ograniczenia aplikacji**.

Atrybut	Opis
Ograniczenia aplikacji	

Blokada nagrywania głosu w aplikacjach	Jeśli jest ustawiony, mikrofon nie może być używany w urządzeniu. Dostępność: Android Samsung SDK
Nie wymuszaj Google Play Protect	Skanowanie Google Play Protect w celu ochrony przed złośliwym oprogramowaniem jest domyślnie włączone. Ta opcja umożliwia wyłączenie skanowania. Wymaga najnowszej wersji Google Play services na Androidach 6.0, 7.0 z aktywnym profilem służbowym. Dostępność: Android
Blokada zmiany ustawień telefonu	Jeśli włączona, uniemożliwia przejście do ustawień telefonu. Dostępność: Android, tryb Device Owner
Wymuszaj automatyczne ustawienie daty i godziny	Automatycznie pobiera dane czasowe z sieci i blokuje możliwość ręcznych zmian.
Wyłącz możliwość modyfikowania kont	Jeśli ustawione, możliwość dodawania, edytowania lub usuwania konta zostanie zablokowana Dostępność: Device Owner
Blokada zarządzania kontami użytkownika	Jeśli włączona, uniemożliwia tworzenie dodatkowych kont użytkowników. Dostępność: Android Samsung z Enterprise SDK od 4.0

4.5.9 Polityka aplikacji

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka aplikacji**.

Atrybut	Opis
Polityka aplikacji	
Polityka aplikacji w trybie Device Owner	Dostępne ustawienia: • "Brak polityki aplikacji" - nie wprowadzi żadnych zmian we wszystkich aplikacjach zdefiniowanych w sekcji "Dozwolone/Blokowane" • "Blokuj aplikacje z listy" - zablokuje wszystkie aplikacje zdefiniowane w sekcji "Dozwolone/Blokowane" • "Zezwalaj tylko na aplikacje z listy" - zezwoli na wszystkie aplikacje zdefiniowane w sekcji "Dozwolone/Blokowane" Dostępność: Urządzenia w trybie Device Owner

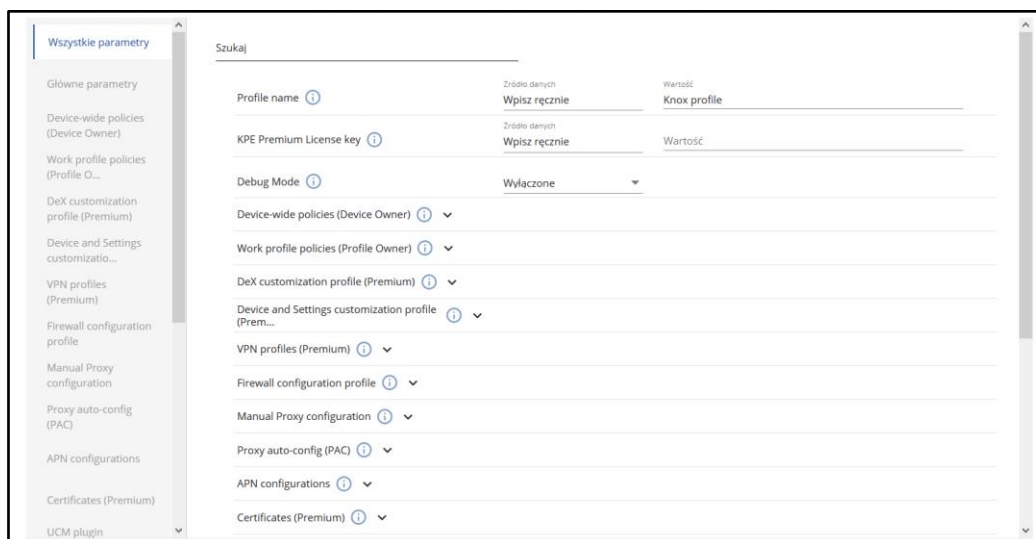
Global polityka uprawnień aplikacji w trybie Device Owner	Dostępne ustawienia: • "Zarządzane przez użytkownika" - pozwala użytkownikowi wybrać, które uprawnienia są zabronione lub dozwolone • "Zezwalaj" - zezwoli na wszystkie uprawnienia dla aplikacji zdefiniowanych w sekcji "Wyjątki uprawnień aplikacji" • "Blokuj" - zablokuje wszystkie uprawnienia dla aplikacji zdefiniowanych w sekcji "Wyjątki uprawnień aplikacji" Dostępność: Urządzenia w trybie Device Owner
Ustawienia automatycznej aktualizacji aplikacji z zarządzanego Google Play	Dostępne ustawienia: • Włącz automatyczne aktualizacje • Włącz automatyczne aktualizacje tylko wtedy, gdy urządzenie jest podłączone do WiFi • Zezwól użytkownikowi urządzenia na konfigurację zasad aktualizacji aplikacji • Wyłącz automatyczne aktualizacje Dostępność: Urządzenia w trybie Device Owner
Dostępność aplikacji w sklepie MGP	Ta opcja określa dostępność aplikacji w Managed Google Store. Można ustawić na: • Tylko włączone aplikacje (domyślnie) – dostępne będą tylko aplikacje włączone i zaakceptowane w Zarządzanym Sklepie Google Play przez FAMOC • Wszystkie aplikacje z Google Play – wszystkie aplikacje są wyświetlane w Zarządzanym Sklepie Google Play i można je instalować

4.5.10 Samsung KSP

Knox Service Plugin (KSP) to rozwiązanie umożliwiające konfigurowanie polityk i zarządzanie urządzeniami mobilnymi obsługującymi platformę Samsung Knox dla przedsiębiorstw (KPE). Procedura konfiguracji KSP opisana jest w osobnym dokumencie dostępnym [tutaj](#).

Ustawienia KSP są częścią sekcji Opcje bezpieczeństwa w szablonie polityk. Aby użyć ustawień KSP w swojej polityce, kliknij opcję Włącz Samsung KNOX Service Plugin. Następnie kliknij Edytuj konfigurację.

KSP zapewnia szereg konfigurowalnych parametrów. Aby ułatwić nawigację po ustawieniach, możesz skorzystać z pola wyszukiwania.



Listę wszystkich dostępnych parametrów można znaleźć tutaj:

<https://docs.samsungknox.com/admin/knox-service-plugin/release-notes.htm>

4.6 Zaawansowane

W zakładce ustawień zaawansowanych można ustawić następujące parametry:

Atrybut	Opis
Zaawansowane ustawienia polityk	
Ilość zapamiętanych sesji Monitora urządzenia	Określa, ile sesji Monitora urządzenia ma być przechowywanych przez FAMOC (1-10) Wartość domyślna: 5
Ilość archiwalnych sesji Monitora urządzenia:	Określa, ile sesji Monitora urządzenia ma być przechowywanych w logach (10-150) Default value: 20
Dane raportowane w sesji Monitora urządzenia	Wybierz, które dane będą raportowane przez monitor użytkownika. Wartość domyślna: Wszystkie (możliwe wybory: parametry podstawowe; aplikacje; Bluetooth; dyski; punkty dostępu; certyfikaty; administratorzy urządzeń; konta na urządzeniu; aktualizacje oprogramowania; karty SIM)
Interwał synchronizacji czasu	Ustawia, jak często zegar systemowy urządzenia S60 jest zsynchronizowany z serwerem Network Time Protocol Wartość domyślna: Wyłączony
Informowanie o zmianie karty SIM (np. podczas kradzieży telefonu)	Tak/Nie Wartość domyślna: Nie

Limit urządzeń na użytkownika	Liczba urządzeń, które użytkownik może dodać za pomocą strony startowej, gdy ustawiana jest opcja autoryzacji użytkownika. Jeśli limit zostanie przekroczony, użytkownik nie może dodawać żadnego innego urządzenia do systemu za pomocą strony startowej.
Nazwa organizacji wyświetlana na urządzeniu	Wprowadzony tekst zostanie wyświetlony na ekranie blokady urządzenia.
Pokaż drugą linię w nagłówku FAMOC Base Agent	Tak lub nie
Wartość drugiej linii w nagłówku FAMOC Base Agent	Pobierane z wybranego pola

Ciągłe raportowanie i ostrzeganie o parametrach

W tej sekcji możesz zdefiniować, które parametry baterii będą raportowane w czasie rzeczywistym. Możesz włączyć raportowanie ciągłe lub szczytowe. Jeśli stan baterii przekroczy określony próg lub status, w konsoli zarządzania FAMOC pojawi się alert.

Dostępne parametry są wymienione poniżej:

- Stan baterii - gdy raportowana wartość różni się od podanej (np. określono: dobry, zaraportowane: przegrzanie)
- Poziom naładowania baterii - gdy raportowana wartość jest niższa niż określona 10%-50%
- Temperatura akumulatora - gdy raportowana wartość jest wyższa niż określone 20-100 stopni Celsjusza
- Napięcie akumulatora - gdy raportowana wartość jest wyższa niż podana 2V-10V
- Stan ładowarki - gdy raportowany stan różni się od podanego (np. określony: Podłączony, raportowany: Brak połączenia)
- Niski poziom baterii - gdy zgłaszana wartość jest równa podanej
- Pamięć RAM Wolna - gdy raportowana wartość jest niższa niż określona (10-50%)
- Siła sygnału - gdy raportowana wartość jest niższa niż określona (np. określona: -80 dBm, raportowana: -107 dBm)

Szczegóły urządzenia w agencie bazowym

Administrator może dodać niestandardowe pola, które będą wyświetlane na karcie **Informacje o urządzeniu**.

Rysunek 21 Pola szczegółów urządzenia

Ustawienia kopii zapasowej

W tej sekcji możliwe jest ustawienie synchronizacji wszystkich kontaktów lub synchronizację danych tylko w grupach, których członkiem jest użytkownik. W przypadku tej drugiej opcji administrator może określić dodatkowe grupy, z których będą zsynchronizowane kontakty. Aby dodać grupy użytkowników do synchronizacji danych kontaktowych, użyj przycisku Wybierz. Możesz także ustawić interwał synchronizacji kontaktów codziennie, co tydzień lub co miesiąc.

Rysunek 22 Ustawienia synchronizacji kontaktów

5. Polityki urządzeń współdzielonych

Zasady dotyczące urządzeń współdzielonych umożliwiają nakładanie ograniczeń na urządzenia działające w trybie współdzielonym.

5.1 Ustawienia podstawowe

Aby dodać ogólny szablon polityk, podaj nazwę i ustaw priorytet.

Atrybut	Opis
Ustawienia podstawowe	
Nazwa szablonu	Wprowadź nazwę polityki (maks. 100 znaków)

Ustaw priorytet	Określ pozycję na liście szablonów
Przeinstaluj Base Agenta automatycznie	Po pojawieniu się w systemie nowej wersji programu Base Agent zostanie ona automatycznie ponownie zainstalowana na urządzeniach (polityka zostanie ustawiona jako nieaktualna). Wartość domyślna: niezaznaczone.
Odinstaluj niezgodne elementy polityki automatycznie	Jeśli ta opcja jest zaznaczona, niepasujące elementy z bieżącej polityki zostaną odinstalowane, jeśli urządzenie zostanie przypisane do innej polityki. Wartość domyślna: niezaznaczone.
Oznacz urządzenie jako wyczyszczone przy wykrytym odinstalowaniu Agenta Bazowego	Jeśli ta opcja jest zaznaczona, urządzenie zostanie oznaczone w konsoli FAMOC jako wyczyszczone w przypadku odinstalowania Agenta Bazowego. Wartość domyślna: niezaznaczone.
Raportowane aplikacje	Dostępne opcje: • Raportuj wszystkie aplikacje • Raportuj tylko zarządzane aplikacje

5.1.1 Ustawienia harmonogramów

Poniżej znajduje się lista parametrów ustawień harmonogramów polityk.

Atrybut	Opis
Ustawienia harmonogramów	
Interwał synchronizacji w szczycie	Interwał połączenia z serwerem Base Agent: 5 min./15 min./30 min./1 g./4 g./12 g./Raz dziennie/Raz w tygodniu/Raz w miesiącu Wartość domyślna: raz dziennie
Dni szczytu	Dni tygodnia, w trakcie których Agent Bazowy raportuje do serwera FAMOC Wartość domyślna: od poniedziałku do piątku
Początek szczytu	O której godzinie w dniach szczytu powinien zacząć raportowanie agent podstawowy Wartość domyślna: 8:00
Koniec szczytu	O której godzinie w dniach szczytu powinien zakończyć raportowanie agent podstawowy Wartość domyślna: 16:00
Interwał sesji Monitora Urządzenia	Ustawia interwał sesji Monitora Urządzenia: Wyłączony/Co godzinę, 4 razy dziennie/Codziennie/Raz w tygodniu/Raz w miesiącu Wartość domyślna: Codziennie

Informowanie o nieaktywności urządzenia	Ostrzeganie o bezczynności agenta bazowego po: 1-5 dniach/tygodniu/miesiącu/3 miesiącach. Jeśli agent bazowy nie połączy się z serwerem w tym okresie, FAMOC wygeneruje alert z trzema możliwymi opcjami reakcji: • Usuń urządzenie z FAMOC • Zainstaluj ponownie program Base Agent • Oznacz urządzenie jako skradzione Wartość domyślna: po tygodniu
Wyczyść urządzenie przy przekroczonej nieaktywności	Jeśli ta opcja jest zaznaczona, a agent bazowy nie zgłasza się do serwera w określonym czasie, oprócz wygenerowanego alertu urządzenie zostanie wyczyszczone.
Oznacz urządzenie jako wyczyszczone przy przekroczonej nieaktywności	W przypadku przekroczenia czasu zgłoszenia się urządzenia do serwera, zostanie ono oznaczone w konsoli FAMOC jako wyczyszczone.

5.2 Przypisane grupy urządzeń

Każda polityka przypisana jest do określonych grup użytkowników lub grup urządzeń, dlatego każde urządzenie otrzymuje ustawienia polityk wstępnie zdefiniowane do przypisanej grupy. Urządzenia nienależące do żadnej grupy oraz grupy, które nie są przypisane do żadnej polityki, otrzymują politykę o najniższym priorytecie (polityka znajdująca się na dole listy). Urządzenia przypisane do kilku grup otrzymują politykę o wyższym priorytecie.

W zakładce **Grupy** administrator może przydzielać grupy do polityk. Aby wybrać grupę, kliknij przycisk **Dodaj grupę urządzeń** lub przycisk **Dodaj grupę użytkowników**. Zostanie wyświetlone okno z listą grup.



Zaznacz pola wyboru obok odpowiednich grup i kliknij **Wybierz**. Grupy zostaną teraz przypisane do polityki.

5.3 Elementy polityki

Oprócz ogólnych ustawień istnieje możliwość dodania konfiguracji i aplikacji do polityki.

Aby dodać konfigurację do polityki, kliknij przycisk **Wybierz konfigurację**. Pojawi się okno z listą konfiguracji.

Konfiguracja może być ustawiona dla:

- Szczytu – konfiguracja zostanie zastosowana w okresie szczytu
- Poza szczytem – konfiguracja zostanie zastosowana poza okresem szczytu
- Zawsze – konfiguracja będzie zawsze stosowana

Za każdym razem, gdy urządzenie łączy się z serwerem, sprawdza, czy zastosowana jest odpowiednia polityka, a jeśli potrzebna jest zmiana (np. zakończył się okres szczytu, a aktualnie stosowana konfiguracja dotyczy tylko tego okresu), stara konfiguracja jest usuwana, a zastosowana jest odpowiednia. Polityki oparte na czasie mogą być stosowane tylko na urządzeniach z systemem iOS.

Aby dodać aplikację, kliknij przycisk **Wybierz aplikację**. Pojawi się okno z listą aplikacji. Wybrane aplikacje zostaną zainstalowane podczas przypisywania polityk do urządzenia. Po zmianie polityk przypisanych do urządzenia zastosowane zostaną nowe polityki i zainstalowana nowa lista aplikacji. Podczas wyboru aplikacji, można określić liczbę powtórzeń instalacji (w przypadku anulowania instalacji przez użytkownika, FAMOC ponowi operację). Możliwe opcje:

- Instalacja obowiązkowa (opcja domyślna) - jeśli instalacja zostanie anulowana, będzie powtarzana co dzień.
- Jedna próba instalacji - jeśli instalacja zostanie anulowana, nie będzie ponawiana.
- Kilka prób instalacji - instalacja będzie ponawiana określoną liczbę razy.

Elementy polityki można ustawić w niestandardowej kolejności instalacji, używając strzałek w dół/w górę w kolumnie **Kolejność**.

Domyślnie każdy element jest instalowany w sekwencji (następny element rozpoczyna się po pomyślnym zainstalowaniu poprzedniego). Można jednak oznaczyć element jako niezależny (kolumna **Niezależny**), co oznacza, że kolejna akcja rozpoczyna się niezależnie od poprzedniej, nie czekając na raport z powodzeniem.

Zaznacz opcję **Ignoruj błąd**, aby wykonać następną akcję, jeśli poprzednia zakończyła się niepowodzeniem.

Elementy polityki		Wybierz aplikację		Wybierz konfigurację	
Nazwa elementu	Akcja	Ignoruj błąd	Niezależny	Kolejność	
Require 4 chars lock code on Android	Polityka szczytu: Zawsze ▾	☐	☐	↓	×
Tapeta FF 1080p	Polityka szczytu: Zawsze ▾	☐	☐	↑	×

5.4 Opcje bezpieczeństwa na urządzeniu

W tym miejscu dostępne są dwie subsekcje:

- Polityka aktualizacji
- Polityka sprzętowa

5.4.1 Polityka aktualizacji

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka aktualizacji**.

Atrybut	Opis
Polityka aktualizacji	
Polityka aktualizacji OTA	Możliwość zdefiniowania polityki aktualizacji OTA. Dostępne opcje to: • Brak polityki • Automatyczna • Według harmonogramu • Wstrzymana Dostępność: Device Owner (blokuje aktualizację systemu na 30 dni), Android Samsung z Enterprise SDK 3.0

5.4.2 Polityka sprzętowa

Poniżej znajduje się lista ustawień dostępnych w zakładce **Polityka sprzętowa**.

Atrybut	Opis
Polityki sprzętowe	
Blokada trybu przeglądania plików USB	Jeśli włączona, nie będzie możliwości przeglądania plików przez połączenie USB.
Blokada trybu awaryjnego	Jeśli opcja zostanie ustawiona, na urządzeniu nie będzie dostępny tryb awaryjny.
Blokada trybu samolotowego	Jeśli opcja zostanie ustawiona, na urządzeniu nie będzie dostępny tryb samolotowy.

5.5 Ustawienia profilu użytkownika

W tym miejscu można określić pewne ograniczenia dla profili tworzonych na urządzeniu współdzielonym.

5.5.1 Ograniczenia profilu do pracy

Atrybut	Opis
Ograniczenia profilu do pracy	
Włączenie instalacji z nieznanymi źródłami	umożliwia lub blokuje możliwość instalowania aplikacji za pośrednictwem plików .apk na profilu służbowym. Zasady nie będą aktywne na urządzeniach z Androidem 5.0 (instalacja .apk jest zablokowana).

Blokada przechwytywanie obrazu	Umożliwia zablokowanie przechwytywania ekranu w aplikacji, która działa w profilu do pracy, aby uniemożliwić udostępnianie danych tą metodą.
Wyłącz możliwość modyfikowania kont	Blokuje możliwość dodawania, edytowania lub usuwania konta. Blokada tworzenia konta email (tylko dla urządzeń Samsung)
Blokada aparatu	Jeśli włączona, wyłącza możliwość korzystania z aparatu.
Wyłącz możliwość kontrolowania aplikacji	Jeśli włączona, użytkownicy nie będą mogli modyfikować aplikacji (odinstalować, zatrzymać działanie, wyczyścić dane aplikacji).

5.5.2 Włączone aplikacje

W tej sekcji Administrator może udostępnić aplikacje systemowe Google w profilu służbowym, aby były automatycznie dostępne dla użytkowników po aktywacji profilu. Udostępnione aplikacje na urządzeniu mogą się różnić, ponieważ niektóre wersje Androida (szczególnie wersje markowe) mogą nie obejmować wszystkich wymienionych aplikacji systemowych. Administrator może zmienić listę włączonych aplikacji i ukryć je zgodnie z potrzebami. Domyślne aplikacje, które są zawsze widoczne po aktywacji profilu, to FAMOC Base Agent i zarządzany sklep Google.

5.6 Zaawansowane

W zakładce ustawień zaawansowanych można ustawić następujące parametry:

Atrybut	Opis
Zaawansowane ustawienia polityk	
Ilość zapamiętanych sesji Monitora urządzenia	Określa, ile sesji Monitora urządzenia ma być przechowywanych przez FAMOC (1-10) Wartość domyślna: 5
Ilość archiwalnych sesji Monitora urządzenia:	Określa, ile sesji Monitora urządzenia ma być przechowywanych w logach (10-150) Default value: 20
Dane raportowane w sesji Monitora urządzenia	Wybierz, które dane będą raportowane przez monitor użytkownika. Wartość domyślna: Wszystkie (możliwe wybory: parametry podstawowe; aplikacje; Bluetooth; dyski; punkty dostępu; certyfikaty; administratorzy urządzeń; konta na urządzeniu; aktualizacje oprogramowania; karty SIM)

Interwał synchronizacji czasu	Ustawia, jak często zegar systemowy urządzenia S60 jest zsynchronizowany z serwerem Network Time Protocol Wartość domyślna: Wyłączony
Informowanie o zmianie karty SIM (np. podczas kradzieży telefonu)	Tak/Nie Wartość domyślna: Nie
Limit urządzeń na użytkownika	Liczba urządzeń, które użytkownik może dodać za pomocą strony startowej, gdy ustawiana jest opcja autoryzacji użytkownika. Jeśli limit zostanie przekroczony, użytkownik nie może dodawać żadnego innego urządzenia do systemu za pomocą strony startowej.
Nazwa organizacji wyświetlana na urządzeniu	Wprowadzony tekst zostanie wyświetlony na ekranie blokady urządzenia.

6. Status polityk na stronie szczegółów urządzenia

Status polityk dotyczących urządzenia można sprawdzić na stronie głównej szczegółów urządzenia lub w zakładce "Polityki".

Na liście polityk wyświetla się:

- **Nazwa** – nazwa polityki
- **Zastosowana** – data przypisania polityki do urządzenia
- **Podgląd polityki** – otwiera okienko z aktualnymi ustawieniami polityki
- **Status** – wyświetla status polityki na urządzeniu. Po najechnięciu myszą na ikonę statusu, wyświetli się lista brakujących elementów polityki
- **Kolumna akcji** – jeśli polityki nie są przypisane lub są nieaktualne, wyświetla link do ręcznego wysłania konfiguracji do urządzenia

Przypisana polityka			
Nazwa polityki	Zastosowana	Podgląd polityki	Status
Mike Secure COPE	2019-09-30 10:29:31		
• Profil do pracy	2019-09-18 15:43:20		
Status Exchange proxy			
Status połączenia			
Ostatnie udane połączenie			
Identyfikator Exchange	815478010878497		



Uruchom Zdalny dostęp

Rysunek 25 Widok przypisanej polityki