techstep

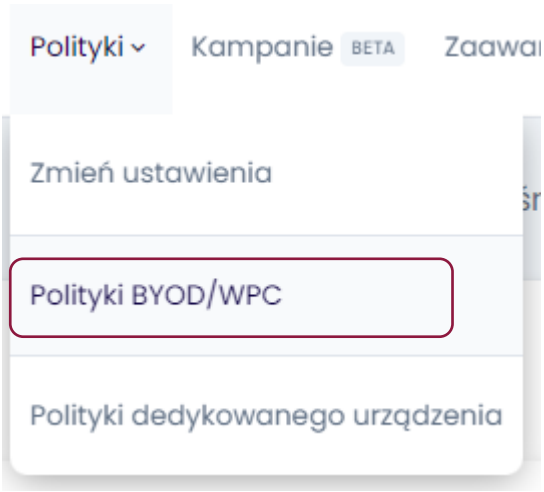
Techstep Essentials MDM

Polityki BYOD/WPC

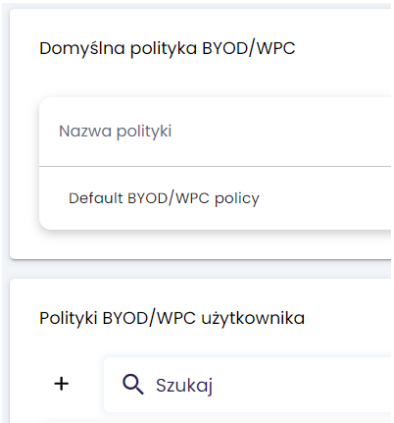
Data: 30/11/2023

Polityki BYOD / WPC

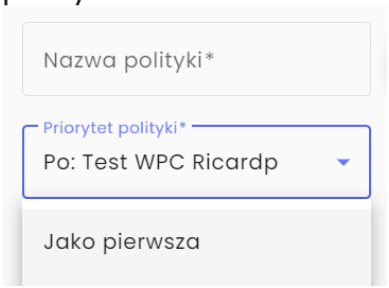
W zakładce polityki znajduje się nowa opcja Polityki BYOD/WPC. W tym miejscu wyświetlana jest lista domyślnych i niestandardowych polityk. W obecnej wersji lista pozwala na dostosowanie kolumn i otwarcie szczegółów polityki.



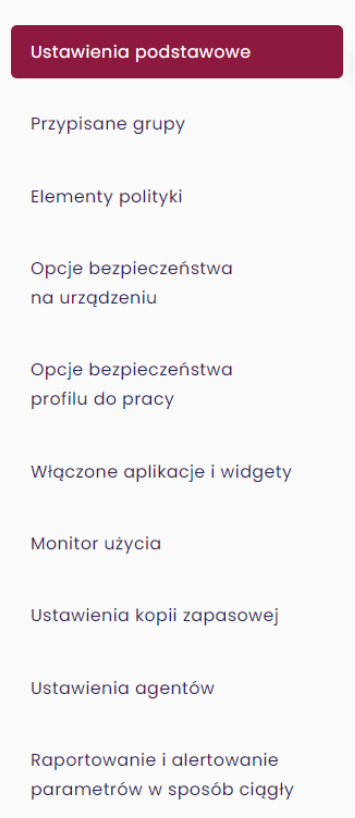
Następnie będziesz musiał wybrać między edycją istniejącej domyślnej polityki lub utworzeniem zupełnie nowej.



Aby utworzyć nową politykę BYOD / WPC, kliknij symbol + po lewej stronie. Podczas tworzenia nowej polityki należy nadać jej nazwę i ustawić priorytet polityki:



Po lewej stronie dostępnych jest kilka opcji:

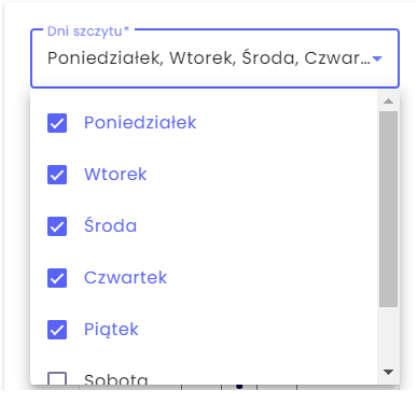


Ustawienia podstawowe

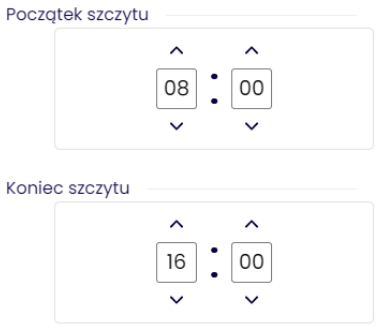
W ustawieniach podstawowych znajdują się następujące opcje:

- Przeinstaluj Base Agenta automatycznie (Tak/Nie)
- Odinstaluj niezgodne elementy polityki automatycznie (Tak/Nie)
- Włącz Samsung Premium API
  - Po ustawieniu wyświetlone zostaną pola: licencja Premium, data wygaśnięcia licencji Premium i dodatkowa opcja Włącz atestację Samsung.
  - Licencja Premium i data wygaśnięcia są wymagane.
- Atestacja SafetyNet
  - Włączenie tej opcji uniemożliwi rejestrację urządzeń z odblokowanym Bootloaderem.
  - Administrator może ustawić interwał atestacji urządzenia.
- Oznacz urządzenie jako wyczyszczone przy odinstalowaniu Base Agenta (Tak/Nie)
- Włącz usługi zdalnego pulpitu (Tak/Nie)
  - Po ustawieniu administrator może ustawić zgodę na inicjalizację sesji zdalnej przy użyciu następujących wartości:
    - Zarządzana przez użytkownika
    - Wymagaj przy każdym połączeniu

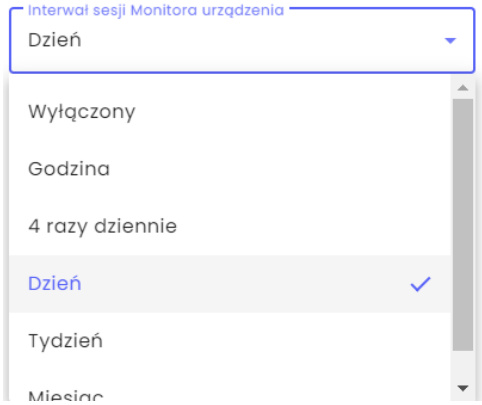
        - Automatyczne połączenie
- Włącz usługi lokalizacyjne (Tak/Nie)
    - Po wybraniu tej opcji administrator może ustawić:
        - Interwał pobierania lokalizacji
        - Wyłącz raportowanie lokalizacji poza szczytem
        - Wyłącz raportowanie lokalizacji po zainstalowaniu agenta
- Ignoruj optymalizację zużycia baterii dla Monitora lokalizacji i Monitora użycia
    - Zaznaczenie tej opcji spowoduje wysłanie operacji, która wymaga potwierdzenia przez użytkownika
- Raportuj dodatkowe informacje o aplikacjach (rozmiar aplikacji, rozmiar pamięci podręcznej, rozmiar danych)
  (Opcja wymaga włączenia uprawnienia Dostęp do danych)
- Raportowane aplikacje (opcja dostępna dla urządzeń iOS)
    - Raportuj wszystkie aplikacje
    - Raportuj wyłącznie aplikacje zarządzane
- Dni szczytu



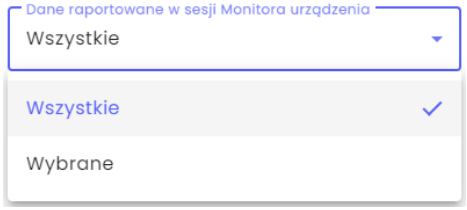
- Czas obowiązywania szczytu



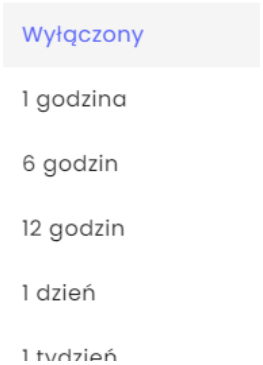
- Interwał sesji Monitora urządzenia



- Ilość zapamiętanych sesji Monitora urządzenia
  - 5-50
- Dane raportowane w sesji Monitora urządzenia (Android)

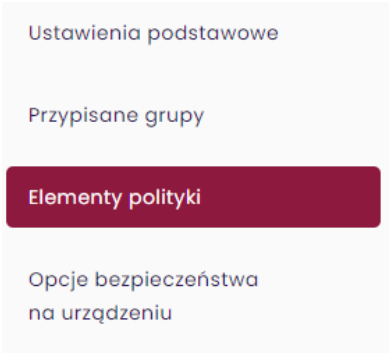


- Wyczyść urządzenie przy przekroczonej nieaktywności (Tak/Nie)
- Oznacz urządzenie jako wyczyszczone przy przekroczonej nieaktywności (Tak/Nie)
- Interwał synchronizacji czasu

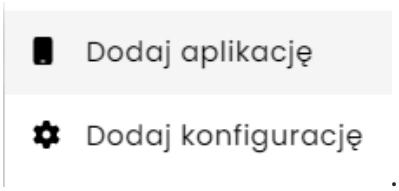


- Informowanie o zmianie karty SIM (np. podczas kradzieży telefonu) (Tak/Nie)
  Numer BRAMKI SMS Serwera (informacja o zmianie karty SIM):
- Limit urządzeń na użytkownika (Wartość numeryczna, 1-999.999)

Elementy polityki



Tutaj możesz dodać komponenty do swojej polityki. Możliwe jest wybranie aplikacji lub konfiguracji.



.

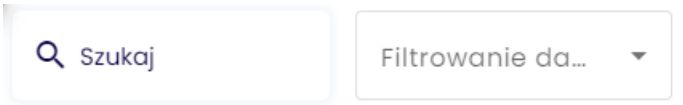
.

Opcje bezpieczeństwa

Opcje bezpieczeństwa są podzielone na "Opcje bezpieczeństwa na urządzeniu" i "Opcje bezpieczeństwa profilu do pracy".

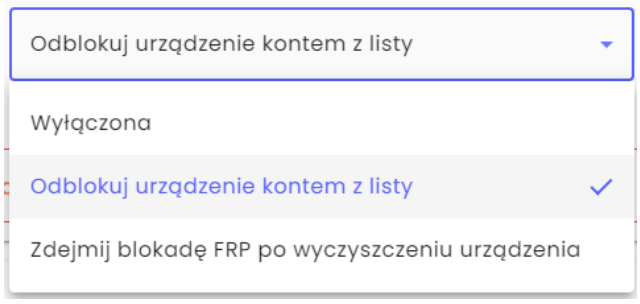
Na urządzeniach BYOD stosowane są tylko opcje zabezpieczeń profilu służbowego, na urządzeniach WPC (profil służbowy na urządzeniach należących do firmy) stosowane są obie opcje.

Istnieje kilka opcji zabezpieczeń, aby zabezpieczyć urządzenia w BYOD/WPC. Można również przeprowadzić wyszukiwanie lub filtrowanie wg trybów lub urządzeń BYOD, WPC, iOS, iPadOS i MacOS.



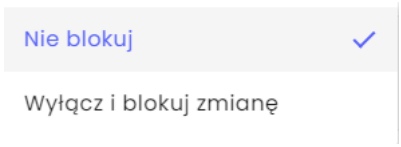
Opcje bezpieczeństwa na urządzeniu

- Polityka czyszczenia danych:
  - Czyszczenie pamięci telefonu po wykryciu zmiany karty SIM (Tak/Nie)
  - Czyszczenie pamięci telefonu na brak karty SIM (Tak/Nie)
    (Czyszczenie pamięci przy zmianie karty SIM musi być włączone)
  - Czyszczenie urządzenia po wykryciu rootowania (Tak/Nie)
  - Ochrona przywracania do ustawień fabrycznych (FRP)

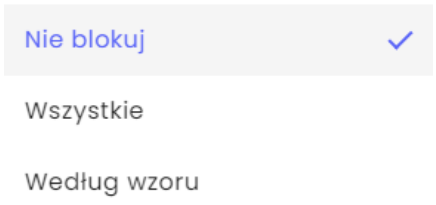


- Polityka sieci:
  - Blokada interfejsu Wi-Fi (Tak/Nie)
  - Blokada ręcznej konfiguracji Wi-Fi (Tak/Nie)
    (Blokada interfejsu Wi-Fi musi być włączona)
  - Zapobiegaj wyłączeniu Wi-Fi (Tak/Nie)
  - Blokada interfejsu Bluetooth (Tak/Nie)

- Blokada danych pakietowych w roamingu



- Blokada rozmów wychodzących



- Blokuj konfigurację Bluetooth (Tak/Nie)
- Blokuj konfigurację udostępniania internetu (Tak/Nie)
- Blokada konfiguracji sieci mobilnych (Tak/Nie)
- Blokada konfiguracji transmisji komórkowej (Tak/Nie)
- Wyłącz wiadomości SMS (Tak/Nie)
- Nie zezwalaj na połączenia komórkowe 2G (Tak/Nie)
- Nie zezwalaj na łącze ultraszerokopasmowe(UWB) (Tak/Nie)

- Polityka lokalizacji:
  - Zablokuj możliwość zmiany ustawień lokalizacji (Tak/Nie)
  - Wyłącz możliwość udostępniania lokalizacji na urządzeniu (Tak/Nie)

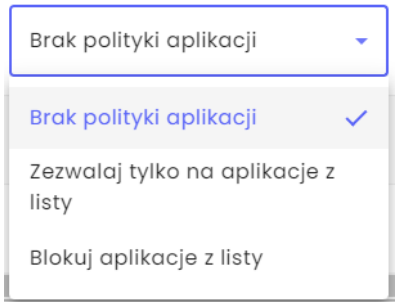
- Polityka aktualizacji
  - Aktualizacje OTA dla urządzeń Zebra (Tak/Nie)

- Polityka sprzętowa
  - Blokada trybu awaryjnego (Tak/Nie)
  - Blokada trybu samolotowego (Tak/Nie)
  - Włącz tryb debugowania USB (Tak/Nie)
  - Blokada przechwytywania obrazu (Tak/Nie)
  - Blokada przesyłania plików po USB (Tak/Nie)
  - Wyłącz możliwość montowania fizycznych nośników zewnętrznych (Tak/Nie)

- Polityka instalatora
  - Blokada nieznanych źródeł (Tak/Nie)

- Ograniczenia aplikacji
  - Blokada nagrywania głosu w aplikacjach na urządzeniu (Tak/Nie)
  - Wymuszaj automatyczne ustawienie daty i godziny (Tak/Nie)

- Polityka aplikacji na urządzeniu WPC



- Wyłącz przechwytywanie treści na urządzeniu (Tak/Nie)
- Wyłącz sugestie dotyczące treści na urządzeniu (Tak/Nie)

Opcje bezpieczeństwa profilu do pracy

- Polityka czyszczenia danych:
  - Usuń dane korporacyjne przy zmianie karty SIM (Tak/Nie) **(WPC/BYOD)**
  - Usuń dane korporacyjne przy wykryciu braku karty SIM (Tak/Nie) **(WPC/BYOD)**
    (Czyszczenie danych przy zmianie karty SIM musi być włączone)
  - Usuń dane korporacyjne po wykryciu rootowania (Tak/Nie) **(WPC/BYOD)**

- Polityka sieci:
  - Wyłącz ustawienia VPN (Tak/Nie) **(WPC/BYOD)**
  - Blokada edycji zarządzanych sieci (Tak/Nie) **(WPC/BYOD)**
  - Monitoruj listę zarządzanych konfiguracji Wifi (Tak/Nie) **(WPC/BYOD)**

- Polityka sprzętowa:
  - Wyłącz Siri (Tak/Nie)
  - Wyłącz Siri kiedy urządzenie jest zablokowane (Tak/Nie)
  - Wyłącz połączenia z serwerami Siri na potrzeby dyktowania (Tak/Nie)
  - Wyłącz połączenia z serwerami Siri na potrzeby tłumaczenia (Tak/Nie)
  - Wyłącz automatyczne przesyłanie raportów diagnostycznych do Apple (Tak/Nie)
  - Wyłącz centrum kontroli na zablokowanym ekranie (Tak/Nie)
  - Nie pozwalaj na kopie zapasowe Enterprise books (Tak/Nie)
  - Nie pozwalaj na synchronizacje meta danych Enterprise Book (Tak/Nie)

    - Wyłącz podgląd historii powiadomień na zablokowanym ekranie (Tak/Nie)
    - Wyłącz podgląd dzisiejszych powiadomień na zablokowanym ekranie (Tak/Nie)
    - Wyłącz użycie iCloud przez zarządzane aplikacje (Tak/Nie)
    - Wymuś użycie hasła do parowania na urządzeniach otrzymujących zadania z tego urządzenia (Tak/Nie)
    - Wymuszenie szyfrowania kopii zapasowej (Tak/Nie)
    - Wymuś rozpoznawanie nadgarstka na Apple Watch (Tak/Nie)
    - Wymuś ustawienie kodu blokady (Tak/Nie)

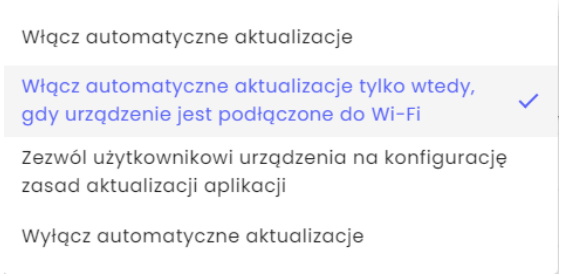
- Polityka szyfrowania pamięci:
    - Szyfrowanie pamięci wewnętrznej (Tak/Nie)

- Polityka instalatora:
    - Blokada instalacji aplikacji (Tak/Nie)
    - Tworzenie kont przez Google Play (Tak/Nie)

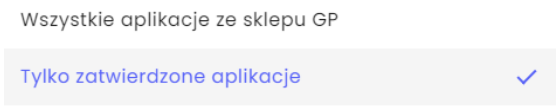
- Ograniczenia aplikacji:
    - Blokada nagrywania głosu w aplikacjach (Tak/Nie)
    - Nie zezwalaj na udostępnianie zarządzanych dokumentów za pomocą AirDrop (Tak/Nie)
    - Nie zezwalaj na udostępnianie danych z niezarządzanych aplikacji (Tak/Nie)
    - Nie zezwalaj na udostępnianie danych z zarządzanych aplikacji (Tak/Nie)
    - Zezwalaj niezarządzanym aplikacjom na czytanie z zarządzanych kont z kontaktami (Tak/Nie)
    - Włącz ograniczenia 'Nie zezwalaj na udostępnianie danych z niezarządzanych/zarządzanych aplikacji' dla funkcji kopiowania i wklejania (Tak/Nie)
    - Wyłącz możliwości odinstalowywania aplikacji (Tak/Nie)
    - Włącz w Safari ostrzeżenia o oszustwach (Tak/Nie)
    - Nie zezwalaj na konfigurowanie domyślnych aplikacji (Tak/Nie)

- Polityka aplikacji:

- Ustawienia automatycznej aktualizacji aplikacji z zarządzanego Google Play

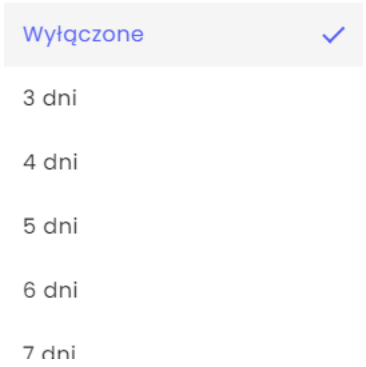


- Dostępność aplikacji w sklepie MGP



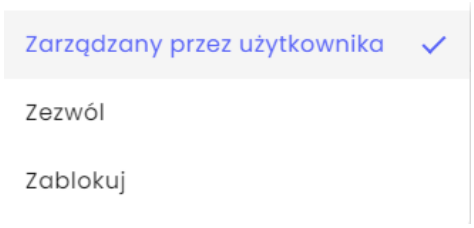
- Ograniczenia profilu do pracy:
  - Włączenie instalacji z nieznanych źródeł (Tak/Nie)
  - Blokada przechwytywania obrazu (Tak/Nie)
  - Wyłącz możliwość modyfikowania kont (Tak/Nie)
  - Blokada tworzenia konta email (Tak/Nie)
  - Blokada tworzenia konta LDAP (Tak/Nie)
  - Blokada tworzenia konta Samsung (Tak/Nie)
  - Blokada aparatu (Tak/Nie)
  - Wyłącz możliwość kopiowania-wklejania w profilu (Tak/Nie)
  - Wyłącz możliwość kontrolowania aplikacji (Tak/Nie)
  - Wyłącz możliwość użycia tej samej blokady dla urządzenia oraz profilu służbowego (Tak/Nie)
  - Zezwalaj na przenoszenie aplikacji do profilu do pracy (Tak/Nie)
  - Blokada NFC (Tak/Nie)
  - Nie zezwalaj na przesyłanie danych za pomocą NFC (Tak/Nie)
  - Zezwalaj na przenoszenie plików z urządzenia do profilu do pracy (Tak/Nie)
  - Zezwalaj na przenoszenie plików z profilu do pracy do urządzenia (Tak/Nie)
  - Blokada zmiany udostępniania kalendarza do trybu osobistego (Tak/Nie)
  - Blokada zmiany udostępniania kalendarza do profilu do pracy (Tak/Nie)
  - Aktywacja interfejsu Bluetooth (Tak/Nie)
  - Włącz udostępnianie plików przez Bluetooth w profilu do pracy (Tak/Nie)
  - Blokada udostępniania przez Share Via List (Tak/Nie)

- Zablokuj konfigurację poświadczeń przez użytkowników w zarządzanym magazynie kluczy (Tak/Nie)
- Maksymalny czas, przez jaki profil do pracy może być wyłączony (3-14 dni)

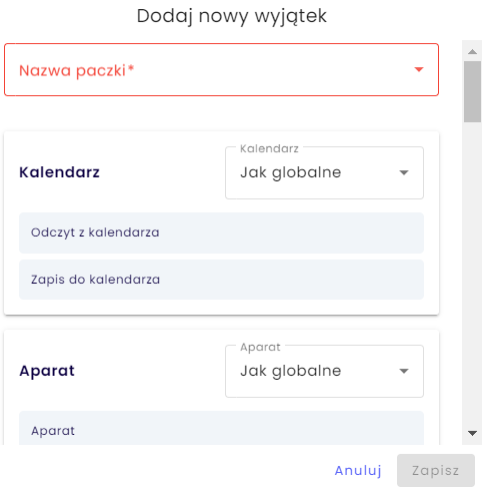


- Włącz możliwość przywrócenia kopii zapasowej z konta Google (Tak/Nie)
- Wyłącz możliwość włączania lokalizacji w ustawieniach (Tak/Nie)
- Wyłącz możliwość udostępniania lokalizacji (Tak/Nie)
- Wyłącz przechwytywanie treści (Tak/Nie)
- Wyłącz sugestie dotyczące treści (Tak/Nie)

- Uprawnienia aplikacji w profilu do pracy:
  - Globalny dostęp aplikacji



  - Wyjątki uprawnień aplikacji
    - Administrator może tworzyć wyjątki do globalnej polityki uprawnień. Dla każdej aplikacji możemy ustawić wyjątki dla poszczególnych kategorii uprawnień:
      - Kalendarz
      - Aparat
      - Kontakty
      - Lokalizacja
      - Mikrofon
      - Telefon
      - Czujniki
      - SMS
      - Pamięć
      - Aktywność fizyczna



- Samsung KSP
  - Włącz Samsung Knox Service Plugin (Tak/Nie)
    - Po ustawieniu możemy dokonać opcjonalnej konfiguracji wtyczki Samsung Knox Service Plugin

Włączone aplikacje i widgety

- Włączone aplikacje – aplikacje dostępne w profilu do pracy po skonfigurowaniu urządzenia, możliwe opcje:
  - Gmail
  - Microsoft Outlook
  - Kalendarz
  - Aparat
  - Galeria
  - Telefon
  - Wiadomości
  - Google Drive
  - Kontakty
  - Pobrane
  - Google Maps
  - Zegar
  - Bixby
  - Samsung Galaxy Store
  - Netflix
  - One Drive
  - Youtube
  - Facebook
  - Google Chrome
  - Pomocnik aplikacji Twój telefon - Łącze do Windows

        - Google Duo
        - Pliki
        - Przeglądarka Samsung Internet
        - Samsung Notes
    - Włączone widgety dla aplikacji w profilu roboczym – lista włączonych widżetów udostępnionych w profilu do pracy

Monitor użycia

- Włącz monitor użycia (Tak/Nie)
  The Android Usage agent monitors and reports user activity to the Essentials MDM server, records outgoing and incoming voice calls, and gives insight into outgoing and incoming text and MMS messages. Essentials MDM Usage Monitor installation is like Base Agent installation.
    - Raportuj dane po restarcie urządzenia (Tak/Nie)
    - Ustawienia danych pakietowych
        - Raportuj użycie danych po Wi-Fi
        - Raportuj użycie danych po GPRS

          Nie raportuj

          Co 15 minut

          Co 30 minut

          Co godzinę

          Co 6 godzin

          Codziennie

          Co 3 dni

          Co tydzień

          Co 2 tygodnie

          Co miesiąc

          Co 3 miesiące
- Ustawienia rozszerzonego raportowania
    - Raportuj stan urządzenia (Tak/Nie)
    - Raportuj czas odblokowania/zablokowania ekranu (Tak/Nie)
    - Raportuj użycie aplikacji (Tak/Nie)
        - Raportuj rozszerzone parametry

Nie raportuj

Co 15 minut

Co 30 minut

Co godzinę

Co 6 godzin

Codziennie

Co 3 dni

Co tydzień

Co 2 tygodnie

Co miesiąc

Co 3 miesiące

Ustawienia kopii zapasowej

- Ustawienia synchronizacji kopii zapasowej
  Obsługiwana jest tylko kopia zapasowa kontaktów
  - Interwał kopii zapasowej

    Wyłączony

    Raz dziennie

    Raz na tydzień

    Raz na miesiąc

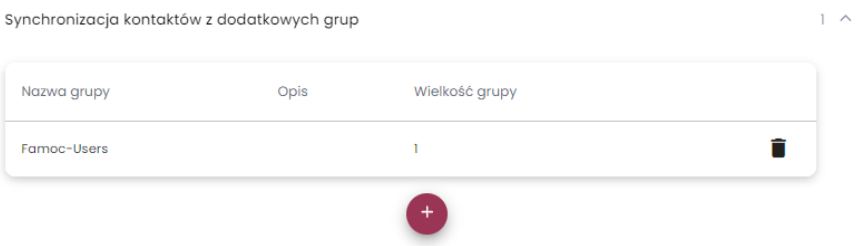
- Synchronizacja kontaktów biznesowych
  - Podstawowy typ synchronizacji

    Żadne kontakty

    Kontakty tylko z grup użytkownika

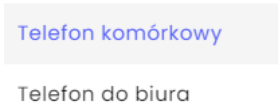
    Kontakty ze wszystkich grup

  - Synchronizacja kontaktów z dodatkowych grup
    Funkcja ta umożliwia dodawanie użytkowników z grup użytkowników w systemie.



- Interwał synchronizacji kontaktów biznesowych

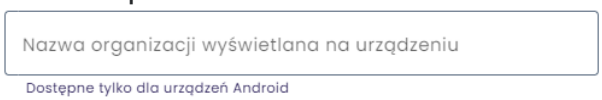
- Domyślny numer kontaktów biznesowych



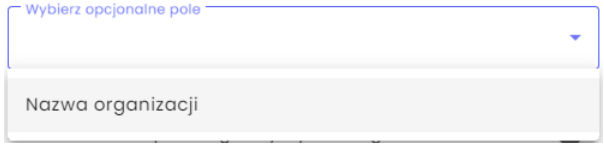
Ustawienia agentów

W tym miejscu można ustawić wybrane wartości, które będą wyświetlane w agencie.

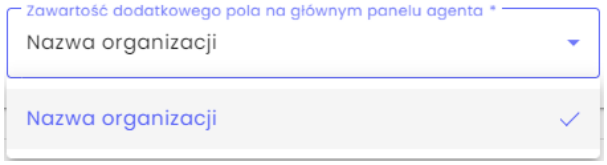
- Nazwa organizacji wyświetlana na urządzeniu
  - Umożliwia skonfigurowanie nazwy organizacji na urządzeniu, np. Techstep.



  - Wybierz pole opcjonalne



- Pokaż dodatkowe pola na panelu głównym agenta (Tak/Nie)
  (Dostępne dla urządzeń z systemem Android i macOS)
  - Zawartość dodatkowego pola na głównym panelu agenta

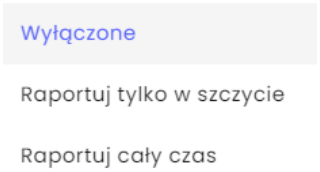


  - Szczegóły urządzenia w agencie (dostępne dla urządzeń z systemem Android i macOS)

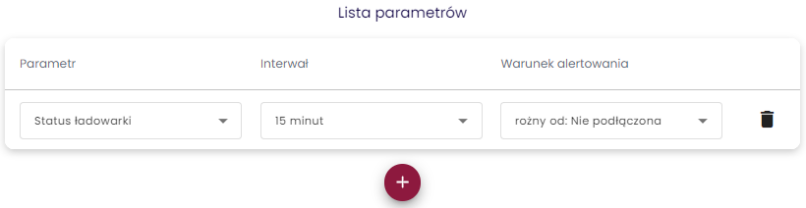
Raportowanie i alertowanie parametrów w sposób ciągły

Funkcja ta umożliwia systemowi raportowanie kilku parametrów z urządzenia, takich jak stan ładowarki, poziom naładowania baterii, wolna pamięć RAM, napięcie baterii, temperatura baterii, stan baterii i niski poziom naładowania baterii.

- Ustawienie raportowania parametrów



  - Raportuj tylko w szczycie



  - Raportuj cały czas