

Przewodnik
zabezpieczeń
Windows Phone 8.1

Spis treści

1.	Wstęp do przewodnika.....	6
2.	Cykl życia urządzeń mobilnych	9
2.1	Rejestracja urządzenia	9
2.2	Zarządzanie konfiguracją urządzenia	9
2.2.1	Konfiguracja zasad.....	9
2.2.2	Zarządzanie przydzielonym dostępem	11
2.2.3	Zarządzanie magazynem	12
2.2.4	Zarządzanie certyfikatami.....	12
2.2.5	Zarządzanie sieciami Wi-Fi.....	13
2.2.6	Zarządzanie połączeniami VPN.....	13
2.2.7	Zarządzanie kontami e-mail	14
2.2.8	Zarządzanie wiadomościami e-mail	14
2.3	Zarządzanie aplikacjami	14
2.4	Zdalna inwentaryzacja i pomoc	15
2.5	Wycofanie urządzenia	16
3.	Przygotowanie do pracy telefonu	17
3.1	Wybór języka urządzenia.....	17
3.2	Akceptacja warunków użytkowania telefonu w zakresie ogólnym oraz zasad zachowania poufności informacji.....	17
3.3	Połączenie urządzenia z siecią do transmisji danych	18
3.4	Czujnik sieci Wi-Fi	19
3.5	Określenie ustawień telefonu w opcji „Zalecane” lub „Dostosuj”	20
4.	Konfiguracja rekomendowanych ustawień zabezpieczeń telefonu z Windows Phone.....	23
4.1	System	23
4.1.1	Ekran + motyw.....	23
4.1.2	Dzwonki + dźwięki.....	24
4.1.3	Poczta + konta	25
4.1.4	Ekran blokady.....	26
4.1.5	Powiadomienia + akcje	28
4.1.6	Wi-Fi.....	28
4.1.7	Tryb samolotowy.....	30

4.1.8	Bluetooth	30
4.1.9	Komórkowe + SIM	31
4.1.10	NFC	32
4.1.11	Udostępnianie Internetu.....	33
4.1.12	VPN.....	34
4.1.13	Kącik z aplikacjami	35
4.1.14	Praca	36
4.1.15	Kącik dziecięcy	37
4.1.16	Oszczędzanie baterii.....	38
4.1.17	Czujnik danych.....	39
4.1.18	Czujnik pamięci.....	39
4.1.19	Jasność	40
4.1.20	Obrót ekranu.....	40
4.1.21	Wyświetl mój ekran.....	40
4.1.22	Znajdź mój telefon.....	41
4.1.23	Kopia zapasowa.....	42
4.1.24	Synchronizacja ustawień	43
4.1.25	Tryb samochodowy	44
4.1.26	Lokalizacja	45
4.1.27	Id. treści reklamowych	45
4.1.28	Data + godzina.....	46
4.1.29	Klawiatura	46
4.1.30	Język	48
4.1.31	Region	48
4.1.32	Raport.....	48
4.1.33	Mowa.....	50
4.1.34	Ułatwienia dostępu.....	51
4.1.35	Aplikacje dla akcesoriów	53
4.1.36	Aktualizacje	54
4.1.37	Informacje	55
4.1.38	Konto Nokia.....	55
4.1.39	Punkt dostępu.....	56
4.1.40	Audio	57

4.1.41	Dotknij	58
4.1.42	Kontrola pamięci	58
4.1.43	Filtr połączeń + SMS	59
4.1.44	Ekran podglądu	59
4.1.45	Wyświetl	60
4.1.46	Sieć +	61
4.1.47	Info + dodatki	61
4.1.48	Koncentrator urządzeń	62
4.1.49	Oceń nas	62
4.2	Ustawienia aplikacji	63
4.2.1	Internet Explorer	64
4.2.1.1	Preferencje witryny internetowej	64
4.2.1.2	Przycisk na pasku adresu kontroluje	65
4.2.1.3	Oszczędzanie w Czujniku danych	66
4.2.1.4	Usuń historię	67
4.2.1.5	Ustawienia zaawansowane	68
4.2.2	Kontakty	71
4.2.3	Mapy	72
4.2.4	Office	73
4.2.5	Portfel	74
4.2.6	Sklep	75
4.2.7	Telefon	77
4.2.8	Wiadomości	79
4.2.9	Wyszukiwanie	80
4.2.10	Zdjęcia + aparat	81
5.	Konfiguracja urządzeń z Windows Phone w środowisku scentralizowanym	84
5.1	Konfiguracja ustawień zabezpieczeń w Windows Intune	84
5.1.1	Ustawienia zabezpieczeń haseł	84
5.1.2	Ustawienia szyfrowania	86
5.1.3	Ustawienia systemu	87
5.1.4	Ustawienia kont i synchronizacji	87
5.1.5	Ustawienia e-mail	87
5.1.6	Ustawienia przeglądarki	88

5.1.7	Ustawienia aplikacji	88
5.1.8	Ustawienia sprzętu	88
5.1.9	Ustawienia funkcji	90
6.	Bezpieczeństwo danych	91
6.1	Szyfrowanie	91
6.1.1	Szyfrowanie magazynu wewnętrznego	91
6.1.2	Ochrona nośników zewnętrznych	92
6.1.3	Zarządzanie prawami do informacji	92
6.1.4	Szyfrowanie i podpisywanie S/MIME	93
6.1.5	Szyfrowanie połączeń	93
6.2	Ochrona przed złośliwym oprogramowaniem	93
6.2.1	Proces uruchamiania systemu	94
6.2.2	Zaufany proces uruchomienia systemu	94
6.2.3	Integralność systemu i aplikacji	94
6.2.4	Sklep	95
6.2.5	Kontener aplikacji	95
6.2.6	Ochrona aplikacji systemu operacyjnego	96
6.2.7	Aplikacje biznesowe	96
6.2.8	Portal firmy	96
6.2.9	Internet Explorer	97
6.3	Kontrola dostępu	97
6.3.1	Dostęp do urządzenia	97
6.3.2	Przypisany dostęp	98
6.3.3	Listy dozwolonych i zabronionych aplikacji	98
6.3.4	Wirtualne karty inteligentne	99
6.3.5	Uwierzytelnianie za pomocą certyfikatów	99
6.3.6	Połączenia VPN	99
6.3.7	Dostęp bezprzewodowy	100
6.3.8	Pomoc zdalna	100
7.	Wycofanie urządzenia z użytku	101
7.1	Bezpieczne usuwanie danych	101
7.2	Przywracanie ustawień fabrycznych	101
7.2.1	Resetowanie urządzenia z poziomu ustawień telefonu	102

7.2.2	Resetowanie urządzenia za pomocą przycisków sprzętowych	102
8.	Spis rysunków	103

1. Wstęp do przewodnika

Wszystkie współczesne organizacje są świadome konieczności zabezpieczania danych przetwarzanych na urządzeniach mobilnych. Z uwagi na ich powszechność stosowania w miejscach publicznych daje to gwarancję minimalizacji ryzyka związanego z ich utratą lub zagubieniem. Dodając rozwiązania centralnego zarządzania i możliwość wsparcia użytkowników na odległość, korzystanie z posiadanych urządzeń zgodnie z inicjatywą Bring Your Own Device (BYOD) wymaga prawidłowego zdefiniowania ustawień zabezpieczeń.

Dodając dynamiczny rozwój systemów zarządzania urządzeniami mobilnymi MDM (Mobile Device Management) łatwo określić trendy rozwoju wiodących modeli zarządzania środowiskami IT.

Platforma Windows Phone posiada pokaźną pulę ustawień, które można z powodzeniem definiować zarówno w rozwiązaniach autonomicznych jak i hybrydowych.

Celem przewodnika jest ukazanie dostępnych możliwości zabezpieczania smartfonów wyposażonych w system Windows Phone 8.1 w kontekście pełnego cyklu życia urządzeń mobilnych.

Firma Microsoft bazując na informacjach przesyłanych przez użytkowników wprowadziła szereg zmian i ulepszeń w systemie Windows Phone 8.1. Wprowadzone modyfikacje sprawiają, że urządzenia wyposażone w system Windows Phone 8.1 są bardziej bezpieczne, łatwiejsze w użytkowaniu oraz to, że współpracują z scentralizowanymi systemami zarządzania w przedsiębiorstwach.

Poniższa tabela przedstawia zmiany dotyczące zabezpieczeń jakie zostały wprowadzone w Windows Phone 8.1

Zmiany w systemie zabezpieczeń	Opis
Bezpieczna rejestracja urządzeń za pomocą systemu MDM.	Urządzenia mogą być rejestrowane w systemach MDM w łatwiejszy i bezpieczniejszy sposób niż w systemie Windows Phone 8. Nowością w Windows Phone 8.1 jest możliwość rejestracji urządzeń w systemach MDM za pomocą uwierzytelniania przez stronę internetową (WAB).
Zarządzanie polisami zabezpieczeń.	Windows 8.1 zawiera szereg ustawień zabezpieczeń, które mogą być zarządzane za pomocą systemu MDM.
Szyfrowanie danych na nośnikach przenośnych.	Windows Phone 8.1 wspiera możliwość instalacji aplikacji na zaszyfrowanych nośnikach zewnętrznych. Dane aplikacji przechowywane są na specjalnie przeznaczonej do tego celu ukrytej partycji. Szyfrowanie partycji aplikacji jak i partycji systemowej może zostać włączone za pomocą systemu MDM.
Zarządzanie aplikacjami.	Windows Phone 8.1 podobnie jak Windows 8.1 zawiera mechanizm, który pozwala na definiowanie listy dozwolonych aplikacji jakie będą używane na urządzeniu.

Wsparcie dla podpisywania i szyfrowania wiadomości e-mail za pomocą protokołu S/MIME.	Windows Phone 8.1 wspiera protokół S/MIME. Za pomocą systemu MDM można zarządzać certyfikatami, które będą używane do podpisywania i szyfrowania wiadomości e-mail wysyłanych z telefonów.
Wsparcie dla łączności z sieciami WiFi w ramach przedsiębiorstw.	Zabezpieczenia łączności WiFi zostały wzbogacone o obsługę: • Extensible Authentication Protocol - Transport Layer Security (EAP-TLS), • EAP-Tunneled Transport Layer Security wireless (EAP-TTLS), • uwierzytelnianie za pomocą certyfikatów. Powyższe metody uwierzytelniania są znacznie bezpieczniejsze w porównaniu do metody uwierzytelniania za pomocą hasła.
Wsparcie dla wirtualnych kart inteligentnych.	Windows Phone 8.1 wspiera wirtualne karty inteligentne, które mogą zapewnić dwustopniowe metody uwierzytelniania (2FA). Wielostopniowe metody potwierdzania poświadczeń są znacznie bezpieczniejsze niż klasyczne metody polegające na podaniu tylko loginu i hasła.
Nowe typu tuneli przy połączeniach VPN	Nowe typy tuneli VPN wprowadzone w Windows Phone 8.1: • Internet Key Exchange Protocol version 2 (IKEv2), • IP security (IPsec), • Secure Sockets Layer (SSL).
Automatyczne nawiązywanie połączeń VPN	Windows Phone może zostać skonfigurowany do automatycznego nawiązywania połączeń VPN w przypadku kiedy określona aplikacja została uruchomiona lub nastąpiło odwołanie do konkretnej domeny.
Pomoc zdalna	Pomoc zdalna jest używana do świadczenia pomocy użytkownikom w rozwiązywaniu problemów z ich urządzeniami. Pomoc jest świadczona na odległość, bez konieczności fizycznego dostępu do urządzenia. Za pomocą tej funkcjonalności można dokonać zdalnie takich czynności jak np.: • zdalne zablokowanie urządzenia, • zdalne wyzwolenie dzwonka urządzenia, • zdalne zresetowanie kodu PIN.
Zdalne wykasowanie danych przedsiębiorstwa	Za pomocą systemu MDM należącego do przedsiębiorstwa istnieje możliwość zdalnego wykasowania wszystkich danych i aplikacji, które

	zostały przesłane do telefonu z systemu przedsiębiorstwa. Dane prywatne użytkownika takie jak muzyka, zdjęcia, prywatne wiadomości e-mail nie są kasowane.
--	--

2. Cykl życia urządzeń mobilnych

Cykl życia urządzeń mobilnych wskazuje fazy, w których wykonywane są różne czynności obsługowe zapewniające prawidłowe funkcjonowanie zarządzanej platformy. Dla środowiska Windows Phone wyróżnia się pięć faz, które przedstawione zostały na poniższym rysunku.



Rys. 1 Fazy cyklu życia platformy Windows Phone

2.1 Rejestracja urządzenia

Rejestracja urządzenia stanowi pierwszą fazę cyklu życia urządzenia i umożliwia obsługę ustawień, zarządzanie aplikacjami oraz ochronę znajdujących się w nim danych.

Rejestracja obejmuje przygotowanie telefonu do pracy i opcjonalne połączenie z systemem zarządzania urządzeniami mobilnymi MDM (Mobile Device Management).

2.2 Zarządzanie konfiguracją urządzenia

Zarządzanie konfiguracją obejmuje wiele obszarów:

- konta e-mail,
- certyfikaty urzędu certyfikatów CA,
- profile sieci Wi-Fi,
- profile wirtualnych sieci prywatnych,
- portal firmowy i inne aplikacje biznesowe LoB (Line of Business),
- zasady.

2.2.1 Konfiguracja zasad

Platforma Windows Phone udostępnia wiele kategorii zasad, które wspierane są przez Microsoft Exchange ActiveSync (EAS). Dzięki temu można z poziomu systemu MDM wysłać ustawienia, które

wykonują zadaną konfigurację. Zasady mogą automatycznie konfigurować urządzenia w oparciu o standardy i polityki zabezpieczeń określone w organizacji.

Windows Phone 8.1 wspiera wszystkie wcześniej dostępne zasady zabezpieczeń oraz zasady zarządzania urządzeniem. Dodatkowo dostępne są nowe zasady, które rozszerzają obszary zarządzania o możliwości:

- wyłączania sklepu Windows Phone,
- wyłączanie możliwości przechwytywania ekranu,
- wyłączanie opcji wycofywania urządzenia z użytku,
- zarządzanie połączeniami W-Fi,
- zarządzanie połączeniami VPN.

Poniższa tabela przedstawia porównanie zasad wspieranych w powiązaniu systemów MDM i EAS oraz w modelu autonomicznym MDM.

Zasada	Exchange	Enterprise Mgmt Server
Wymagaj hasła do odblokowania urządzeń przenośnych	Tak	Tak
Zezwalaj na proste hasła	Tak	Tak
Wymagany typ hasła	Tak	Tak
Minimalna długość hasła	Tak	Tak
Minimalna liczba zestawów znaków	Tak	Tak
Wygaśnięcie hasła w dniach	Tak	Tak
Pamiętaj historię haseł	Tak	Tak
Liczba dopuszczalnych nieudanych logowań przed skasowaniem danych urządzenia	Tak	Tak
Liczba minut braku aktywności przed wyłączeniem ekranu	Tak	Tak
Włączona usługa IRM	Tak	No
Zdalne wykasowanie zawartości telefonu.	Tak	Tak
Wymagaj szyfrowania na urządzeniu przenośnym	Tak	Tak
Zabroń dostępu do karty pamięci	Tak	Tak
Zdalna aktualizacja aplikacji LOB	niedostępne	Tak
Lokalne lub zdalne usunięcie powiązania z usługą MDM	niedostępne	Tak
Odblokowanie w trybie deweloperskim	niedostępne	Tak
Zezwalaj na używanie konta Microsoft do uwierzytelniania w	niedostępne	Tak

ramach połączeń i usług nie obsługujących adresu e-mail jako formy uwierzytelnienia. (nowe w Windows Phone 8.1)		
Zezwalaj na ręczne dodanie konta niepowiązanego z Microsoft.	niedostępne	Tak
Zezwalaj na używanie sklepu z aplikacjami	niedostępne	Tak
Zasady	Exchange	Enterprise Mgmt Server
Blokada wskazanych aplikacji (nowe w Windows Phone 8.1)	niedostępne	Tak
Zezwalaj na komunikację NFC	niedostępne	Tak
Zezwalaj na ręczną instalację certyfikatów głównych	niedostępne	Tak
Zezwalaj na Wi-Fi offloading	niedostępne	Tak
Zezwalaj na raportowanie o dostępnych punktach Wi-Fi hotspot (nowe w Windows Phone 8.1)	niedostępne	Tak
Zezwalaj na ręczną konfigurację ustawień WIFI (nowe w Windows Phone 8.1)	niedostępne	Tak
Zezwalaj na używanie telemetrii (nowe w Windows Phone 8.1)	niedostępne	Tak
Zezwalaj na raportowanie o dostępnych punktach Wi-Fi hotspot (nowe w Windows Phone 8.1)	niedostępne	Tak
Zezwalaj na kopiowanie i wklejanie	niedostępne	Tak
Zezwalaj na połączenie Bluetooth	Tak	Tak
Zezwalaj na udostępnianie połączenia internetowego (nowe w Windows Phone 8.1)	Tak	Tak
Zezwalaj na używanie kamery (nowe w Windows Phone 8.1)	Tak	Tak

W połączeniu z systemem MDM urządzenia Windows Phone 8.1 otrzymują ustaloną konfigurację ustawień i zasad pod warunkiem połączenia do sieci Internet.

2.2.2 Zarządzanie przydzielonym dostępem

Zarządzanie przydzielonym dostępem umożliwia określenie zbioru ustawień i aplikacji dla użytkownika, dzięki czemu można ograniczyć dostęp do wybranych funkcjonalności. Funkcja

przydzielonego dostępu ogranicza również określone funkcje sprzętowe w urządzeniu. Przykładowe scenariusze obejmują:

- dostęp do wybranej aplikacji,
- centralny wykaz dozwolonych i zablokowanych aplikacji,
- konfiguracja dostępu do aplikacji wbudowanych,
- ochrona urządzenia przed uruchamianiem aplikacji, które dają dostęp do informacji poufnych.

2.2.3 Zarządzanie magazynem

Windows Phone 8.1 wykorzystuje funkcję BitLocker Drive Encryption do szyfrowania wewnętrznych magazynów urządzenia. Dzięki temu dane przedsiębiorstwa są zawsze chronione przed nieupoważnionymi osobami nawet w przypadku fizycznego posiadania urządzenia.

W ramach Windows Phone 8.1 można instalować aplikacje na kartach SD (Secure Card) na specjalnie w tym celu wydzielanej partycji. Podobnie jak w przypadku magazynów wewnętrznych stosowane jest szyfrowanie za pomocą klucza AES o długości 128 bitów. Funkcjonalność instalacji aplikacji na kartach SD jest zawsze włączona co zapewnia odpowiedni poziom ochrony.

Zaszyfrowana partycja na karcie SD jest unikalnie wiązana z urządzeniem przez co aplikacje i inne dane znajdujące się w magazynie nie mogą być używane na innym urządzeniu. Dane pozostające na części niezaszyfrowanej mogą być używane na różnych urządzeniach. Stosując zasadę zabraniającą dostępu do karty pamięci można zapobiec wykorzystywaniu kart SD.

2.2.4 Zarządzanie certyfikatami

Certyfikaty mają obecnie bardzo szerokie zastosowanie i są wykorzystywane w takich scenariuszach jak:

- uwierzytelnianie konta,
- uwierzytelnianie Wi-Fi,
- szyfrowanie VPN,
- szyfrowanie zawartości Web za pomocą SSL.

W związku z tym dystrybucja i zarządzanie cyklem życia certyfikatów stanowi strategiczny element dostępności usług, z których korzystają użytkownicy urządzeń mobilnych. Pomimo istnienia opcji ręcznego importu certyfikatów w Windows Phone zalecane jest zarządzanie certyfikatami z poziomu systemu MDM. Wykorzystywanie systemu MDM do zarządzania certyfikatami obejmuje pełny cykl życia certyfikatów – od rejestrowania, przez odnawianie po usunięcie. Windows Phone wykorzystuje protokół SCEP (Simple Certificate Enrollment Protocol) do rejestrowania certyfikatów co umożliwia wykorzystywanie dowolnego urzędu CA.

Dodatkowo Windows Phone zawiera zaawansowane opcje zarządzania certyfikatami oparte na pełnym zestawie interfejsu programistycznego aplikacji API (Application Programming Interface), który jest wykorzystywany przez systemy MDM lub aplikacje firm trzecich. Na przykład, system może korzystać z tych funkcji do archiwizacji szyfrowania Secure/Multipurpose Internet Mail Extensions (S/MIME) i podpisywania certyfikatów dla ich późniejszego wykorzystania w procesie odszyfrowywania niezależnie od używanego urządzenia.

Urządzenia z Windows Phone chronią również klucze do podpisywania i szyfrowania certyfikatów za pomocą wbudowanego w nie modułu TPM (Trusted Platform Module). Wymaga to tylko od użytkownika wprowadzenia kodu PIN do autoryzacji dostępu do kluczy certyfikatów, co dodatkowo zabezpiecza urządzenie, umożliwiając wieloskładnikowe uwierzytelnianie. Na przykład, można użyć tej funkcji do wdrożenia rozwiązania wirtualnych kart inteligentnych. Uwaga: Klucz PIN wymagany do dostępu do certyfikatów w module TPM jest inny niż hasło PIN używane do odblokowywania urządzenia.

Zarządzanie certyfikatami przez system MDM jest transparentne dla użytkowników i nie wymaga z ich strony interwencji. Użytkownicy mogą ręcznie instalować certyfikaty, jednakże realizacja tego za pośrednictwem systemu MDM pomaga zwiększyć efektywność pracy użytkowników jak i zmniejszyć nakłady ze strony zespołu wsparcia technicznego.

2.2.5 Zarządzanie sieciami Wi-Fi

Użytkownicy wykorzystują połączenia bezprzewodowe równie często jak komunikację komórkową. W niektórych scenariuszach sieci Wi-Fi są bardziej preferowane a ich konfiguracja stanowi jeden z ważniejszych elementów zarządzania urządzeniami mobilnymi.

Stosując w zarządzaniu rozwiązanią MDM dostępne są poniższe opcje:

- konfiguracja profili Wi-Fi,
- dostarczanie certyfikatów dla sieci wykorzystujących do uwierzytelniania EAP – TLS (Extensible Authentication Protocol - Transport Layer Security) oraz EAP – TTLS (Tunneled Transport Layer Security),
- wyłączenie udostępniania Internetu przez sieć Wi-Fi,
- wyłączenie Wi-Fi offloading,
- wyłączenie ręcznej konfiguracji profili Wi-Fi,
- wyłączenie raportowania Hotspot Wi-Fi,
- nie używaj sieci Wi-Fi do odciążania transmisji danych.

2.2.6 Zarządzanie połączeniami VPN

W wielu organizacjach istnieje potrzeba zapewnienia zdalnego dostępu do wewnętrznej infrastruktury. Bezpieczeństwo takich połączeń staje się kluczowe. Windows Phone wspiera rozwiązania VPN innych producentów jak i własne rozwiązania w tym zakresie. Dodatkowo w środowisku Windows Phone 8.1 zostało dodane wsparcie dla protokołu IKE (Internet Key Exchange Protocol) w wersji 2, obsługa IPsec oraz połączeń SSL VPN. Dodatkowo wspierane jest automatyczne wyzwalanie połączeń VPN.

Istnieje możliwość tworzenia połączeń VPN dla każdej aplikacji, która potrzebuje nawiązać bezpieczne połączenie z wymaganymi zasobami. Przełączając się między aplikacjami Windows Phone 8.1 automatycznie ustanawia połączenia VPN wymagane przez aplikację.

Uwaga: w danym momencie może być aktywne wyłącznie pojedyncze połączenie VPN.

W przypadku utraty połączenia Windows Phone automatycznie nawiązuje ponowne połączenie bez konieczności interakcji ze strony użytkownika.

Wsparcie dla połączeń VPN ze strony rozwiązań MDM obejmuje:

- konfigurację i aktualizację profili połączeń VPN, włącznie z rodzajem połączenia VPN oraz poświadczeniami,
- powiązanie połączeń VPN z aplikacjami,
- zasadę pozwalającą na wyłączenie połączeń VPN w roamingu,
- zasadę umożliwiającą wyłączenie VPN w sieci komórkowej.

2.2.7 Zarządzanie kontami e-mail

Kluczową usługą w urządzeniach jest poczta elektroniczna. Dostęp do niej stanowi niezbędne ogniwo prowadzenia działań biznesowych. W środowisku Windows Phone istnieje możliwość konfiguracji wielu kont e-mail dla użytkownika, a przy wsparciu systemu MDM pojawia się również możliwość centralnego zarządzania kontami. Dostępne są ustawienia pozwalające na wysyłanie określonych ustawień do urządzenia tak samo jak i opcja zablokowania dodawania kont prywatnych. Dzięki tym funkcjom urządzenie może być używane w określonych przez organizację celach, jednocześnie chroniąc użytkowników przed złośliwym oprogramowaniem pochodzącym z niezabezpieczonych kont pocztowych.

2.2.8 Zarządzanie wiadomościami e-mail

Zarządzanie ustawieniami i wiadomościami e-mail jest możliwe dzięki usługom EAS (Exchange ActiveSync), które zapewniają odpowiednią współpracę z Microsoft Exchange Server. Zarówno w konfiguracji autonomicznej EAS jak i w połączeniu z rozwiązaniem MDM istnieje wiele ustawień pozwalających dopasować wymagania bezpieczeństwa organizacji w kontekście wiadomości e-mail. Poniższa tabela przedstawia listę ustawień w obydwu wymienionych konfiguracjach.

Zasady wspierane przez MDM i EAS	Zasady email wspierane tylko przez EAS
Zezwalaj na proste hasła	Uwzględnij wcześniejsze element email (czas)
Wymagany typ hasła	Uwzględnij wcześniejsze elementy kalendarza (czas)
Minimalna długość hasła	Ograniczenie rozmiaru treści wiadomości
Minimalna liczba zestawów znaków	Ograniczenie rozmiaru treści wiadomości HTML
Wygaśnięcie hasła w dniach	Wymagaj podpisanych wiadomości S/MIME
Pamiętaj historię haseł	Wymagaj zaszyfrowanych wiadomości S/MIME
Liczba dopuszczalnych nieudanych logowań przed skasowaniem danych	Wymagaj podpisanego algorytmu S/MIME
Liczna minut braku aktywności przed wyłączeniem ekranu	Wymagaj zaszyfrowanego algorytmu S/MIME
Wymagaj szyfrowania na urządzeniu przenośnym	Zezwalaj na negocjację algorytmów szyfrowania S/MIME
Zezwalaj na używanie magazynu wymiennego	Zezwalaj na S/MIME SoftCerts
Zezwalaj na używanie kamery	
Zezwalaj na połączenia Bluetooth	
Zezwalaj na sieć Wi-Fi	
Zezwalaj na synchronizację za pomocą USB	

2.3 Zarządzanie aplikacjami

Utrzymanie aplikacji należy do głównych zadań zespołów odpowiedzialnych za urządzenia mobilne i stanowi ważny element kompleksowego rozwiązania zabezpieczeń w organizacji. W środowisku Windows Phone istnieje możliwość wdrażania oprogramowania standardowo dostępnego w sklepie

Microsoft jak i nie publikowanego w nim (tzw. aplikacje ładowane bezpośrednio). Aplikacje ładowane bezpośrednio muszą być podpisane certyfikatem przedsiębiorstwa aby mogły być wdrażane. Certyfikat przedsiębiorstwa musi być zainstalowany na urządzeniu, na którym aplikacja będzie pracowała. W przypadku stosowania rozwiązania MDM wspierane są metody zapewniające wdrażanie i aktualizowanie obydwu rodzajów aplikacji. Aplikacje mogą być oznaczane jako obowiązkowe (wymagane do instalacji) oraz dostępne (instalowane na żądanie użytkownika). Dodatkowo istnieje możliwość usuwania aplikacji bez konieczności interakcji ze strony użytkownika. System MDM zapewnia możliwość standaryzacji dostępnego oprogramowania wg zadanego wykazu (zasada listy aplikacji zezwolonych i listy aplikacji zabronionych). Dostępna jest także zasada blokująca użycie przeglądarki Internet Explorer.

2.4 Zdalna inwentaryzacja i pomoc

W środowisku Windows Phone dostępna jest funkcja zdalnej inwentaryzacji i pomocy. Pozwala to na zarządzanie urządzeniami na odległość a tym samym gwarantuje ciągłość ich utrzymania.

Zdalna inwentaryzacja zapewnia zbieranie parametrów Windows Phone 8.1, które są przedstawione w poniższej. Dzięki dostępowi do danych sprzętowych jak i programowych ułatwiona jest analiza informacji o zasobach urządzeń jak i śledzenie statusu aktualizacji.

Windows Phone 8 i Windows Phone 8.1	Nowe informacje w Windows Phone 8.1
Zainstalowane aplikacje przedsiębiorstwa	Numer telefonu
Nazwa urządzenia	Status połączeń w roamingu
Identyfikator urządzenia	IMEI & IMSI
Rodzaj platformy systemu operacyjnego	Adres IP połączenia Wi-Fi
Wersja oprogramowania układowego	Przyrostek DNS i maska podsieci połączenia Wi-Fi
Wersja systemu operacyjnego	
Czas na urządzeniu	
Typ procesora	
Model urządzenia	
Producent urządzenia	
Architektura procesora zainstalowanego w urządzeniu	
Język interfejsu zainstalowany na urządzeniu	
Adres fizyczny (MAC) karty Wi-Fi zainstalowanej w urządzeniu	

Zdalna pomoc dla Windows Phone gwarantuje możliwość uzyskania wsparcia bez konieczności fizycznego dostępu do urządzenia. Do funkcji zdalnej pomocy zaliczają się:

- Zdalne blokowanie w przypadku zagubienia telefonu lub jego utraty
- Zdalne resetowanie hasła telefonu w przypadku zapomnienia kodu PIN bez ryzyka skasowania danych
- Zdalne wywołanie dźwięku dzwonka urządzenia, dzięki czemu odnalezienie telefonu staje się łatwiejsze

2.5 Wycofanie urządzenia

Ostatnią fazą cyklu życia urządzenia mobilnego jest wycofanie go z użytku. Wiąże się to z koniecznością trwałego usunięcia z telefonu danych przedsiębiorstwa. W przypadku scenariuszy BYOD proces wycofania urządzenia jest bardziej skomplikowany z uwagi na wymóg pozostawienia danych prywatnych użytkownika.

Jeśli urządzenie zostaje zagubione lub skradzione usunięcie danych przedsiębiorstwa musi być wykonane zdalnie z uwagi na ryzyko fizycznego dostępu do telefonu. W środowisku Windows Phone zarządzanym z systemu MDM istnieje opcja zdalnego wymazania zawartości urządzenia, która obejmuje wykasowanie:

- kont e-mail,
- certyfikatów przedsiębiorstwa,
- profili sieciowych,
- wdrożonych aplikacji,
- danych powiązanych z wdrożonymi aplikacjami,
- przekazanych zasad do urządzenia.

W zakresie zarządzania wycofaniem urządzeniem dostępne są zasady zapewniające:

- wyłączenie przez użytkownika możliwości usunięcia powiązania urządzenia z systemem MDM,
- wyłączenie przez użytkownika możliwości programowego i sprzętowego resetowania urządzenia do ustawień fabrycznych.

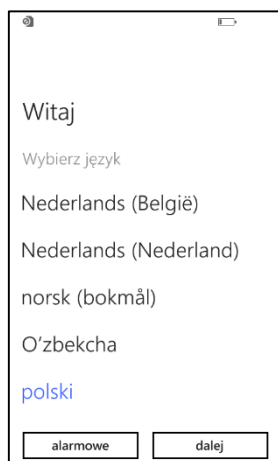
Po wycofaniu urządzenia przez użytkownika do systemu MDM trafia stosowna informacja, która umożliwia wykonanie w razie potrzeby dodatkowej analizy.

3. Przygotowanie do pracy telefonu

Urządzenie wyposażone w system Windows Phone po pierwszym uruchomieniu wymaga przygotowania. W poszczególnych etapach wykonywane są konfiguracje umożliwiające ustawienie urządzenia oraz dostosowanie preferencji osobistych użytkownika.

3.1 Wybór języka urządzenia

Wybór języka urządzenia ma na celu określenie preferencji dzięki czemu korzystanie z telefonu jest dostosowane do potrzeb użytkownika.



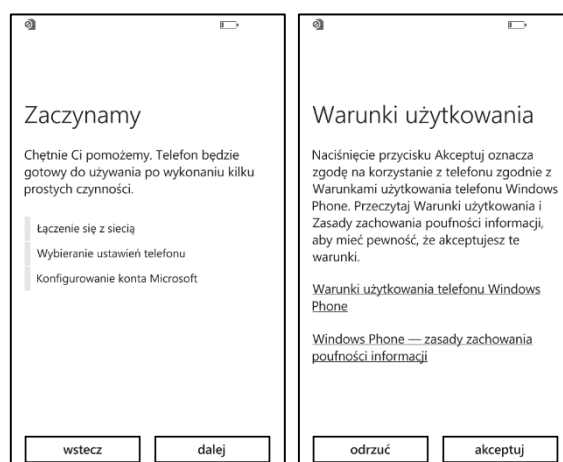
Rys. 2 Okno *Wybierz język*

Ocena ryzyka

Istnieje wiele dostępnych języków dla urządzeń z systemem Windows Phone. Wybór języka nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

3.2 Akceptacja warunków użytkowania telefonu w zakresie ogólnym oraz zasad zachowania poufności informacji

Ogólne warunki użytkowania urządzenia oraz zasady zachowania poufności omawiają wykorzystanie informacji osobistych w celu właściwego działania używanych funkcji oraz dostarczania usługi lub przeprowadzania transakcji żądanych lub autoryzowane przez użytkownika. Zaleca się szczegółowe zapoznanie z treścią postanowień gdyż dostęp do telefonu wymaga ich akceptacji.



Rys. 3 Okno **Zaczynamy** i **Warunki użytkowania**

Ocena ryzyka

Akceptacja warunków użytkownika telefonu nie ma wpływu na ustawienia zabezpieczeń. Stanowi natomiast zbiór ważnych informacji, które mają odniesienie do konfiguracji ustawień na już działającym urządzeniu.

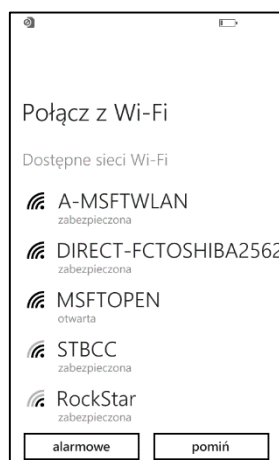
Minimalizacja ryzyka

W celu minimalizacji ryzyka zaleca się dokładnie zapoznanie z zasadami poufności informacji w systemie Windows Phone.

Szczegółowe informacje dostępne są pod adresem <http://www.windowsphone.com/pl-PL/legal/wp8/windows-phone-privacy-statement>.

3.3 Połączenie urządzenia z siecią do transmisji danych

Telefony z systemem Windows Phone mogą nawiązywać połączenia różnego rodzaju, które umożliwiają transmisję danych i komunikację z Internetem oraz z innymi urządzeniami. Podstawowymi sposobami łączności wykorzystującymi transmisję danych są połączenia Wi-Fi oraz łączność komórkowa.



Rys. 4 Okno **Połącz z Wi-Fi**

Ocena ryzyka

- Decydując się na połączenie urządzenia z siecią należy przestrzegać ogólnych zasad bezpieczeństwa.
- Praca w sieciach nieznanach może narazić użytkownika na monitorowanie wykonywanych czynności przez osoby postronne a w efekcie dostęp do przesyłanych oraz przechowywanych danych.

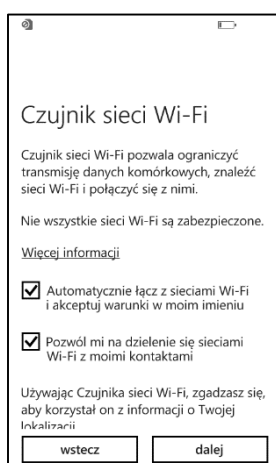
Minimalizacja ryzyka

Przed wszystkim należy pamiętać, że sieci otwarte Wi-Fi nie są bezpieczne. Na przykład każdy może uzyskać z nimi połączenie i potencjalnie monitorować, co w nich jest wykonywane. Należy zachować ostrożność podczas wykonywania w Internecie czynności wymagających wprowadzania danych osobowych lub poufnych. Czynności te najlepiej wykonywać w zaufanej, zabezpieczonej sieci. Konfigurując telefon do pracy z sieciami Wi-Fi należy korzystać w pierwszej kolejności ze znanych sieci zabezpieczonych. W przypadku korzystania z sieci otwartych należy unikać wprowadzania danych osobowych lub poufnych.

3.4 Czujnik sieci Wi-Fi

Czujnik sieci Wi-Fi służy do automatycznego nawiązywania połączenia z pobliskimi sieciami Wi-Fi, umożliwiając w razie potrzeby ograniczenie transmisji danych w sieci komórkowej. Udostępnia również więcej opcji dotyczących połączenia internetowego. Czujnik sieci Wi-Fi może ułatwić łączenie się z sieciami Wi-Fi, wykonując wiele różnych czynności — takich jak:

- automatyczne nawiązywanie połączenia ze znanymi, otwartymi sieciami Wi-Fi, które zostały udostępnione przez innych użytkowników,
- akceptowanie warunków sieci Wi-Fi w imieniu użytkownika telefonu oraz dostarczanie dodatkowych informacji sieciom, które ich wymagają,
- dzielenie się siecią Wi-Fi zabezpieczoną hasłem z kontaktami w celu uzyskania lub nadania dostępu do Internetu bez udostępniania haseł sieciowych.



Rys. 5 Okno konfiguracji **Czujnik Wi-Fi**

Ocena ryzyka

- Wykorzystywanie funkcji **Czujnik sieci Wi-Fi** umożliwia nawiązywanie połączeń z sieciami otwartymi Wi-Fi. Wiąże się to z narażeniem użytkownika na monitorowanie jego aktywności sieciowej, przekazywanie danych osobowych w celu akceptacji warunków podłączenia do sieci otwartych oraz dostarczanie innych, wymaganych do nawiązania połączenia informacji. Dodatkowo wymagany jest dostęp do danych lokalizujących użytkownika.

Minimalizacja ryzyka

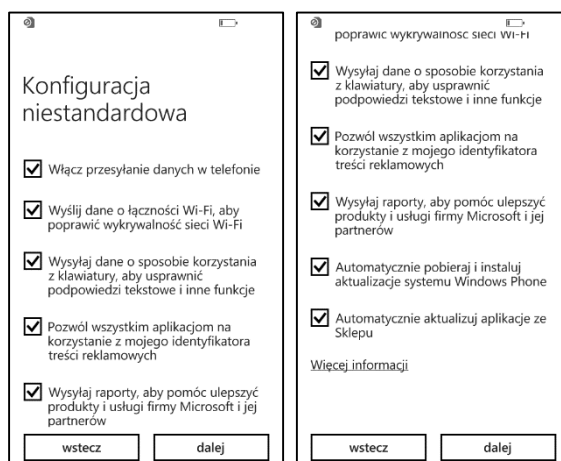
W celu minimalizacji ryzyka zaleca się wyłączyć opcji **Czujnik sieci Wi-Fi** oraz edukowanie użytkowników w zakresie zagrożeń płynących z wykorzystywania sieci otwartych.

3.5 Określenie ustawień telefonu w opcji „Zalecane” lub „Dostosuj”

Podczas pierwszego konfigurowania telefonu zostaną wyświetlone monity o wybranie kilku ustawień telefonu. Do wyboru są dwa tryby: „Zalecane” lub „Dostosuj”. W przypadku trybu **Zalecane** wszystkie poniżej ustawienia mają status Włączone. Tryb **Dostosuj** umożliwia pojedyncze określenie statusu każdego ustawienia.



Rys. 6 Okno wyboru ustawień telefonu – zalecane / dostosuj



Rys. 7 Okno niestandardowej konfiguracji urządzenia

Czas i region

Skąd jesteś?

Polska

W której strefie czasowej jesteś?

(UTC+01:00) Sarajewo, Skopje, Warsz

Data

2014-12-02

Godzina

20:05

☒ Wysyłaj moją lokalizację do firmy Microsoft, gdy telefon jest włączony

[Więcej informacji](#)

alarmowe dalej

Rys. 8 Okno wyboru ustawień *Czas i region*

Zapisywanie w Zrzutach ekranu...

**Ty i Twój świat.
Zawsze razem.**

Konto Microsoft ułatwia nam personalizowanie produktów Microsoft pod Twoim kątem. Dzięki niemu Twoje zdjęcia, kontakty, utwory, dokumenty, ustawienia, hasła, ulubione aplikacje i inne dane są też synchronizowane z komputerem lub konsolą Xbox. Potrzebujesz go również do kupowania aplikacji oraz tworzenia kopii zapasowych i przywracania danych w telefonie.

utwórz konto załoguj

alarmowe

Rys. 9 Okno połączenia urządzenia z kontem Microsoft

Aplikacje

Instalowanie aplikacji w toku. Potrwa to już tylko chwilę.

alarmowe dalej

Prawie gotowe...

Telefon jest prawie skonfigurowany. Ustawienia wymaga teraz aktywowania telefonu. Pomożemy Ci w tym.

dalej

Dziękujemy za wybranie firmy Nokia

Kontynuując, akceptujesz [Warunki świadczenia usług Nokia](#) i [Zasady ochrony prywatności](#). Gwarancja zostanie wysłana do firmy Nokia po połączeniu się z Internetem. Może obowiązywać opłata za przesyłanie danych.

☒ Dołącz do Programu ulepszania produktów firmy Nokia

Dane o użytkowaniu telefonu należące do firmy Microsoft będą współdzielone i łączone z danymi firmy Nokia.

Następnie możesz zacząć korzystać z telefonu — w tym czasie w tle pewne aplikacje będą kończyć instalację.

akceptuj

Rys. 10 Okna finalizacji ustawień

Ocena ryzyka

- Konfiguracja ustawień w opcji Zalecane powoduje włączenie wielu komponentów. Decydując się na taką konfigurację należy przestrzegać ogólnych zasad bezpieczeństwa.

- Praca w sieciach nieznanych może narażać użytkownika na monitorowanie wykonywanych czynności przez osoby postronne a w efekcie dostęp do przesyłanych oraz przechowywanych danych. Wykorzystywanie funkcji Czujnik sieci Wi-Fi umożliwia nawiązywanie połączeń z sieciami otwartymi Wi-Fi. Wiąże się to z narażeniem użytkownika na monitorowanie jego aktywności sieciowej, przekazywanie danych osobowych w celu akceptacji warunków podłączenia do sieci otwartych oraz dostarczanie innych, wymaganych do nawiązania połączenia informacji. Dodatkowo wymagany jest dostęp do danych lokalizujących użytkownika.
- Zgadając się na udostępnianie identyfikatora treści reklamowych aplikacjom zezwalamy na gromadzenie informacji personalizujących użytkownika co wiąże się z wyrażeniem zgody na przekazywanie danych osobowych.
- Włączenie raportów o działaniu systemu Windows Phone powoduje prowadzenie audytu o sposobie korzystania z telefonu, aplikacji oraz generowanych błędach. Wiąże się to z wyrażeniem zgody przez użytkownika na monitorowanie jego aktywności.

Minimalizacja ryzyka

W celu minimalizacji ryzyka zaleca się wyłączenie niepotrzebnych funkcji.

4. Konfiguracja rekomendowanych ustawień zabezpieczeń telefonu z Windows Phone

4.1 System

W ramach sekcji możliwe jest szczegółowe konfigurowanie ustawień systemu Windows Phone.

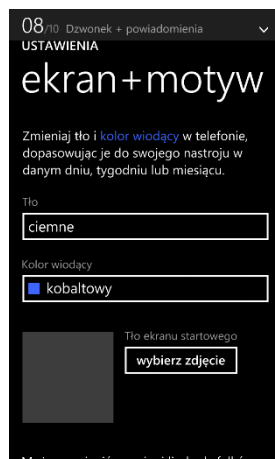


Rys. 11 Ustawienia systemu Windows Phone

4.1.1 Ekran + motyw

W ramach dostępnych opcji można ustawić:

- tło,
- kolor wiodący,
- tło ekranu startowego,
- rozmiar i liczbę kafelków na ekranie startowym.



Rys. 12 Opcje ustawień **Ekran + motyw**

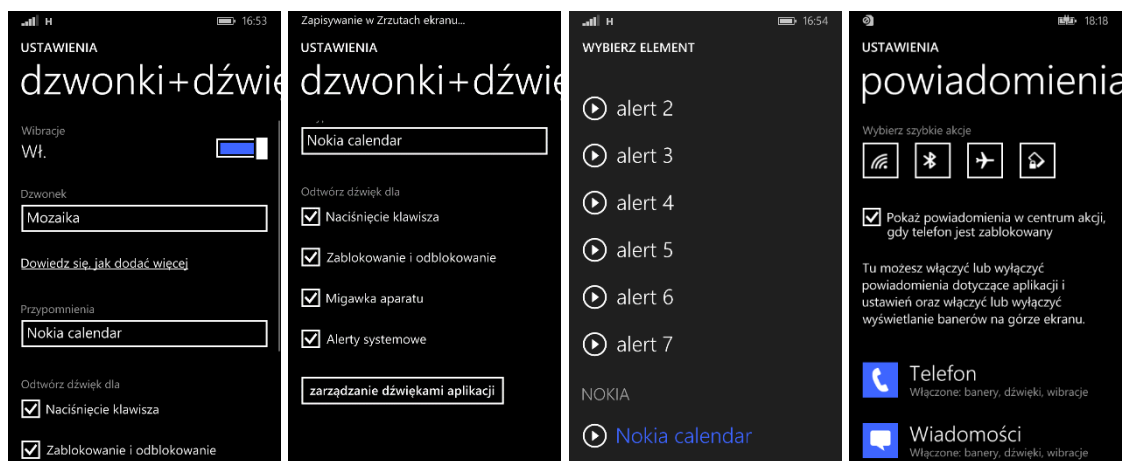
Ocena ryzyka

Wybór ustawień w ramach sekcji **Ekran + motyw** nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.2 Dzwonki + dźwięki

W sekcji **Dzwonki + dźwięki** można dokonać konfiguracji:

- wibracji,
- dzwonka,
- dźwięku przypomnień,
- ustawień odtwarzania dźwięków dla różnych scenariuszy obsługi urządzenia,
- ustawień dźwięków powiadomień dotyczących aplikacji i ustawień,
- włączenia powiadomień w centrum akcji gdy telefon jest zablokowany.



Rys. 13 Opcje ustawień **Dzwonki + dźwięki**

Ocena ryzyka

- Wybór ustawień dotyczący dźwięków nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.
- W przypadku powiadomień związanych z działaniem aplikacji istotne staje się ustawienie czy będą one wyświetlane kiedy urządzenie jest zablokowane.

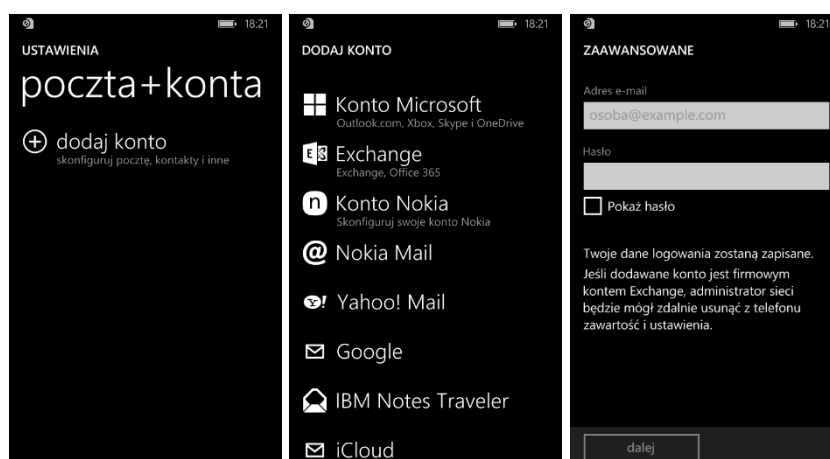
- Włączenie opcji **Pokaż powiadomienia w centrum akcji, gdy telefon jest zablokowany** może przyczynić się do ujawnienia informacji osobom postronnym ponieważ mimo zablokowania urządzenia są one przez krótki czas wyświetlane na ekranie telefonu.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Pokaż powiadomienia w centrum akcji, gdy telefon jest zablokowany	Wł. Wył.	Wł.	Wył.

4.1.3 Poczta + konta

W ramach ustawień sekcji **Poczta + konta** można wykonywać konfigurację kont według predefiniowanych ustawień (Exchange, Outlook.com, Konto Nokia, Nokia Mail, Yahoo Mail, Google, IBM Notes Traveler, iCloud, Facebook, Twitter, LinkedIn, Sina Weibo, konto POP i IMAP) jak i w opcji zaawansowanej umożliwiającej dowolne dostosowanie ustawień.



Rys. 14 Opcje ustawień **Poczta + konta**

Ocena ryzyka

Ustawienia kont mają bezpośredni wpływ na poziom zabezpieczenia telefonu. Związane jest to kilkoma aspektami obejmującymi:

- ustawienia częstotliwości pobierania nowej zawartości,
- dostępu do nazw użytkowników,
- ustawienia dotyczące szyfrowania dla poczty wychodzącej oraz przychodzącej,
- zawartość do synchronizowania,
- ustawienia okresu pobierania wiadomości do urządzenia,
- ustawienia wymagania uwierzytelniania dla serwera poczty wychodzącej,
- wykorzystania tej samej nazwy użytkownika i hasła do wysyłania poczty e-mail.

W zależności od wybranych ustawień istnieje ryzyko dostępu do wiadomości przez osoby niepowołane w przypadku fizycznego dostępu do urządzenia jak również możliwość uzyskania

historii korespondencji jeśli telefon ma aktywne połączenie z siecią. Pominięcie ustawień dotyczących konieczności szyfrowania i wymogu uwierzytelniania może umożliwić przechwycenie korespondencji lub możliwość podszywania się pod tożsamość prawdziwego użytkownika.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Pobierz nową zawartość	po odebraniu na podstawie sposobu używania co 15 minut co 30 minut co godzinę ręcznie	na podstawie sposobu używania	na podstawie sposobu używania
Pobierz pocztę e-mail z	ostatnich 3 dni ostatnich 7 dni ostatnich 2 tygodni ostatniego miesiąca dowolnego okresu	ostatnich 7 dni	ostatnich 7 dni
Zawartość do synchronizowania	Poczta e-mail Kontakty Kalendarz Zadania	Poczta e-mail Kontakty Kalendarz Zadania	Poczta e-mail Kontakty Kalendarz Zadania
Serwer wymaga połączenia szyfrowanego (SSL)	Wł. Wył.	Wł.	Wł.
Serwer poczty wychodzącej wymaga uwierzytelnienia	Wł. Wył.	Wł.	Wł.
Użyj tej samej nazwy użytkownika i hasła do wysyłania poczty e-mail	Wł. Wył.	Wł.	Wł.
Wymagaj SSL dla poczty przychodzącej	Wł. Wył.	Wył.	Wł.
Wymagaj SSL dla poczty wychodzącej	Wł. Wył.	Wył.	Wł.

4.1.4 Ekran blokady

Ustawienia umożliwiają konfigurację opcji odpowiedzialnych za blokowanie ekranu. Należą do nich:

- obraz tła,
- opcja wyświetlania wykonawcy podczas odtwarzania muzyki,
- ustawienia aplikacji w zakresie wyświetlania szczegółowego stanu,
- określenie czasu po jakim wyłącza się automatycznie ekran,
- opcja włączenia zabezpieczenia ekranu hasłem,
- ustawienia wymagania hasła po określonym czasie.



Rys. 15 Opcje ustawień *Ekran blokady*

Ocena ryzyka

- Korzystanie z urządzenia bez opcji blokowania ekranu w przypadku dostępu do niego przez osoby niepowołane wiąże się z ujawnieniem informacji i danych, które znajdują się w telefonie.
- Korzystanie z opcji wyświetlania szczegółowe stanu oraz krótkiego stanu może umożliwić dostęp do poufnych danych nawet przy zablokowanym urządzeniu.

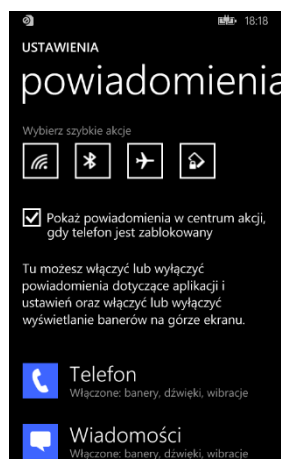
Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Pokaż wykonawcę podczas odtwarzania muzyki	Wł. Wył.	Wył.	Wył.
Wybierz aplikację do wyświetlania szczegółowego stanu	brak Kalendarz Telefon Wiadomości Inne aplikacje w zależności od konfiguracji urządzenia	Kalendarz	brak
Wybierz aplikację do wyświetlania krótkiego stanu	brak Kalendarz Telefon Wiadomości Inne aplikacje w zależności od konfiguracji urządzenia	Telefon Wiadomości	brak
Ekran wyłącza się, kiedy minie	30 sekund 1 min 3 minuty 5 minut	1 min	30 sekund
Hasło	Wł. Wył.	Wył.	Wł.
Wymagaj hasła po	za każdym razem 30 sekund	za każdym razem	za każdym razem

	1 min 3 minuty 5 minut 15 minut 30 minut		
--	--	--	--

4.1.5 Powiadomienia + akcje

W sekcji **Powiadomienie + akcje** można dokonać konfiguracji powiadomień w centrum akcji gdy telefon jest zablokowany.



Rys. 16 Opcje ustawień **Dzwonki + dźwięki**

Ocena ryzyka

- W przypadku powiadomień związanych z działaniem aplikacji istotne staje się ustawienie czy będą one wyświetlane kiedy urządzenie jest zablokowane.
- Włączenie opcji **Pokaż powiadomienia w centrum akcji, gdy telefon jest zablokowany** może przyczynić się do ujawnienia informacji osobom postronnym ponieważ mimo zablokowania urządzenia są one przez krótki czas wyświetlane na ekranie telefonu.

Minimalizacja ryzyka

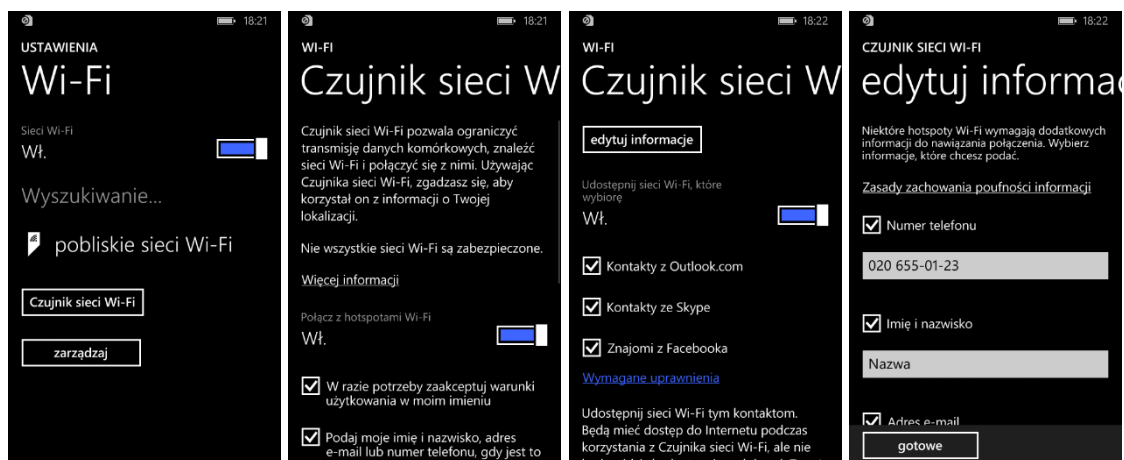
Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Pokaż powiadomienia w centrum akcji, gdy telefon jest zablokowany	Wł. Wył.	Wł.	Wył.

4.1.6 Wi-Fi

Opcja umożliwia włączenie karty bezprzewodowej telefonu oraz konfigurację czujnika sieci Wi-Fi wraz z możliwością zarządzania ustawieniami dodatkowymi.

Istnieje możliwość pomocy użytkownika telefonu w gromadzeniu danych zawierających pobliskie punktu dostępne do sieci Wi-Fi. W przypadku używania tej funkcji wysyłane są (wyłącznie przez sieć Wi-Fi dzięki czemu nie są ponoszone dodatkowe koszty) do firmy Microsoft informacje obejmujące nazwę sieci, jakość połączenia, przepustowość, typ uwierzytelniania i inne szczegóły o sieciach Wi-Fi, z którymi telefon się łączy. Firma Microsoft nie zbiera żadnych danych osobowych

w celu identyfikacji użytkowników, nie wykorzystuje informacji o lokalizacji do śledzenia użytkowników ani nie udostępnia zebranych danych żadnym partnerom. Niezależnie od wyboru ustawienia istnieje możliwość dostępu do danych zebranych przez innych użytkowników telefonów z systemem Windows Phone.



Rys. 17 Opcje ustawień Wi-Fi i Czujnik sieci Wi-Fi

Ocena ryzyka

- Korzystanie z sieci bezprzewodowych zapewnia ciągły dostęp do usług, z których korzystają użytkownicy urządzeń mobilnych.
- W przypadku sieci otwartych (niezabezpieczonych) należy mieć świadomość mogących funkcjonować w nich rozwiązań, których celem jest analizowanie i przechwytywanie ruchu. To z kolei przy połączeniach nieszyfrowanych niesie poważne ryzyko dostępu do przesyłanych danych użytkownika.
- Stosowanie czujnika sieci Wi-Fi pozwala ograniczyć transmisję danych w sieciach komórkowych ale wiąże się z włączeniem opcji lokalizacji. Dodatkowo w przypadku korzystania z sieci otwartych i czujnika danych może nieść ryzyko przekazywania imienia, nazwiska, adresu e-mail lub numeru telefonu do akceptacji dołączenia się do sieci.
- W ramach ustawień istnieje również możliwość udostępnienia sieci Wi-Fi, które wybierze użytkownik innym osobom na podstawie dostępu do kontaktów zgromadzonych w urządzeniu. W zależności od przepisów ogólnych i/lub zasad organizacji może to wiązać się z nieuprawnionym przekazywaniem danych osobowych.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Sieci Wi-Fi	Wł. Wył.	Wył.	Wył.
Połącz z hotspotami	Wł. Wył.	Wł.	Wył.
W razie potrzeby zaakceptuj warunki użytkowania w moim imieniu	Wł. Wył.	Wł.	Wył.

Podaj imię i nazwisko, adres e-mail lub numer telefonu, gdy jest to wymagane	Wł. Wył.	Wł.	Wył.
Udostępnij sieci Wi-Fi, które wybiorę	Wł. Wył.	Wł.	Wył.
Kontakty z Outlook.com	Wł. Wył.	Wł.	Wył.
Kontakty ze Skype	Wł. Wył.	Wł.	Wył.
Znajomi z Facebooka	Wł. Wył.	Wł.	Wył.
Czujnik sieci Wi-Fi wymaga uprawnień użycia Twojego konta na Facebooku	Wł. Wył.	Wył.	Wył.

4.1.7 Tryb samolotowy

Tryb samolotowy umożliwia szybkie wyłączenie:

- łączności komórkowej,
- Wi-Fi,
- radio FM
- Bluetooth,
- udostępnianie NFC.



Rys. 18 Opcje ustawień **Tryb samolotowy**

Ocena ryzyka

Wybór ustawień w ramach **Tryb samolotowy** nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.8 Bluetooth

Ustawienia w sekcji **Bluetooth** umożliwiają:

- włączenie połączeń Bluetooth,

- ręczne parowanie z urządzeniami,
- określenie innego urządzenia Bluetooth dla funkcji Mowa.



Rys. 19 Opcje ustawień **Bluetooth**

Ocena ryzyka

Korzystanie z połączeń Bluetooth w Windows Phone umożliwia wykonywanie wielu czynności, taki jak:

- korzystanie z funkcji Mowa do głosowego wybierania numerów za pośrednictwem zestawu słuchawkowego lub systemu głośnomówiącego w samochodzie,
- wykorzystywanie Cortany w samochodzie,
- udostępnianie plików,
- korzystanie z trybu samochodowego w telefonie,
- parowanie telefonu z określonymi akcesoriami z funkcją NFC,
- odtwarzanie muzyki przez głośniki lub słuchawki Bluetooth, w samochodzie lub przez głośniki komputera,
- odsłuchiwanie odebranych wiadomości SMS i dyktowanie odpowiedzi na nie.

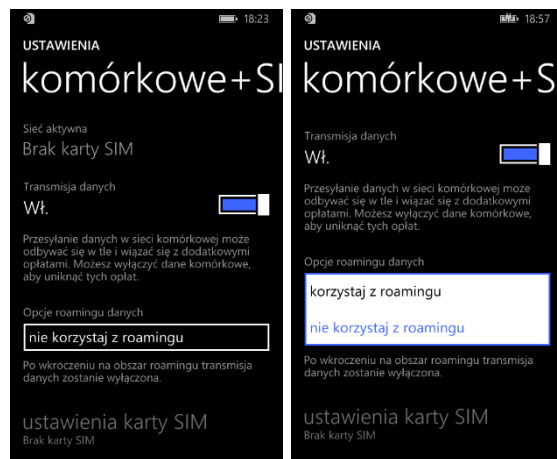
Z uwagi na powyższe w przypadku korzystania z połączeń Bluetooth należy mieć na uwadze to, że mogą funkcjonować rozwiązania, których celem jest analizowanie i przechwytywanie ruchu a tym samym zdalne wpływanie na urządzenia, które korzystają z połączeń Bluetooth.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Stan	Wł. Wył.	Wył.	Wył.
Użyj innego połączenia audio Bluetooth dla funkcji Mowa	Wł. Wył.	Wył.	Wył.

4.1.9 Komórkowe + SIM

Ustawienia sekcji umożliwiają uzyskanie informacji o aktywnej sieci komórkowej, określenie stanu transmisji danych, opcji roamingu danych oraz dokonanie ustawień karty SIM.



Rys. 20 Opcje ustawień **Komórkowe + SIM**

Ocena ryzyka

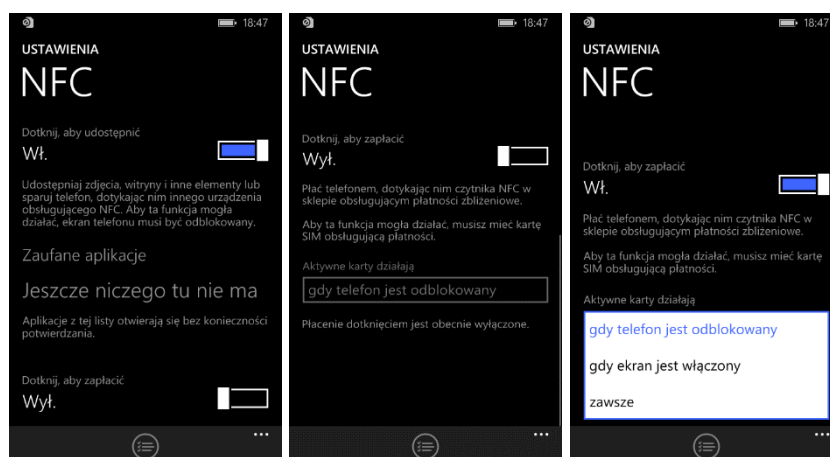
- Włączenie transmisji danych umożliwia działanie wielu funkcji telefonu (np. lokalizacja, odbieranie i wysyłanie poczty e-mail) i niejednokrotnie staje się niezbędne aby móc w pełni korzystać z urządzenia.
- Włączenie opcji lokalizacji zwiększa transfer danych oraz powoduje, że dane osobiste są wysyłane z urządzenia do źródeł korzystających z omawianych opcji.
- W przypadku korzystania z transmisji danych w roamingu istnieje ryzyko narażenia właściciela urządzenia na duże koszty.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Transmisja danych	Wł. Wył.	Wł.	Wył.
Opcje roamingu danych	nie korzystaj z roamingu korzystaj z roamingu	nie korzystaj z roamingu	nie korzystaj z roamingu

4.1.10 NFC

Komunikacja zbliżeniowa **NFC** (Near Field Communication) umożliwia szybkie, bezprzewodowe przesyłanie plików i innych informacji na niewielkie odległości.



Ocena ryzyka

- Komunikacja NFC wymaga bardzo niewielkiej odległości pomiędzy urządzeniami ale osoba postronna może manipulować przesyłane między dwoma urządzeniami NFC dane poprzez próbę ich zakłócania lub niszczenia.
- Istnieje ryzyko przechwytywania danych między dwoma urządzeniami NFC co może spowodować ich rejestrowanie, przekazanie do niepowołanych odbiorców lub modyfikowanie w celu zafałszowania oryginalnych danych.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Udostępniij zdjęcia, strony internetowe i inne dane oraz paruj telefon, dotykając nim innego urządzenia z NFC.	Wł. Wył.	Wył.	Wył.
Płać telefonem, dotykając nim czytnika NFC w sklepie obsługującym płatności zbliżeniowe.	Wł. Wył.	Wył.	Wył.
Aktywne karty działają	gdy telefon jest odblokowany gdy ekran jest włączony zawsze	gdy telefon jest odblokowany	gdy telefon jest odblokowany

4.1.11 Udostępnianie Internetu

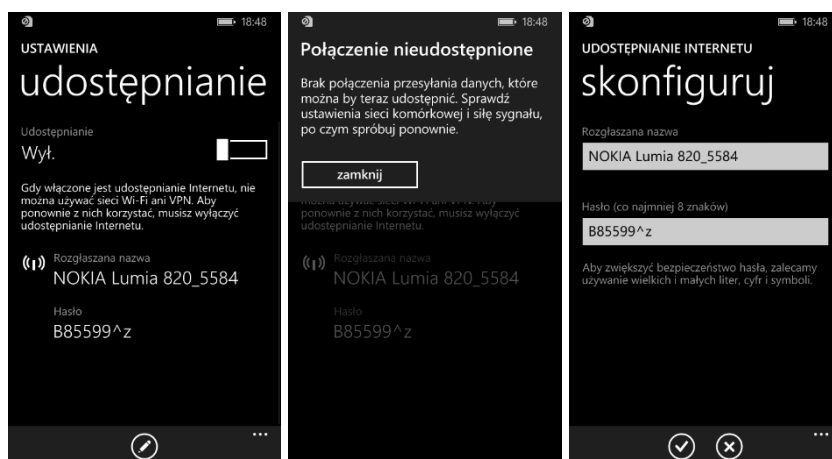
Opcja umożliwia utworzenie mobilnego punktu dostępu do Internetu, który pozwala na udostępnianie połączenia przesyłania danych za pośrednictwem sieci Wi-Fi. Dzięki temu inne urządzenia obsługujące łączność bezprzewodową mogą łączyć się z Internetem.

Ocena ryzyka

- Korzystając z funkcji **Udostępnianie Internetu** należy mieć na uwadze to, że mogą funkcjonować rozwiązania, których celem jest analizowanie i przechwytywanie ruchu a tym samym zdalne wpływanie na urządzenia, które korzystają z udostępnianego połączenia.
- Włączenie opcji **Udostępnianie Internetu** zwiększa transfer danych.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Udostępnienie	Wł. Wył.	Wył.	Wył.
Hasło	-	-	minimum 8 znaków



Rys. 22 Udostępnienie połączenia Internetowego

4.1.12 VPN

Usługa VPN umożliwia nawiązywanie bezpiecznego połączenia z siecią firmową lub Internetem za pośrednictwem sieci Wi-Fi lub połączenia danych komórkowych.

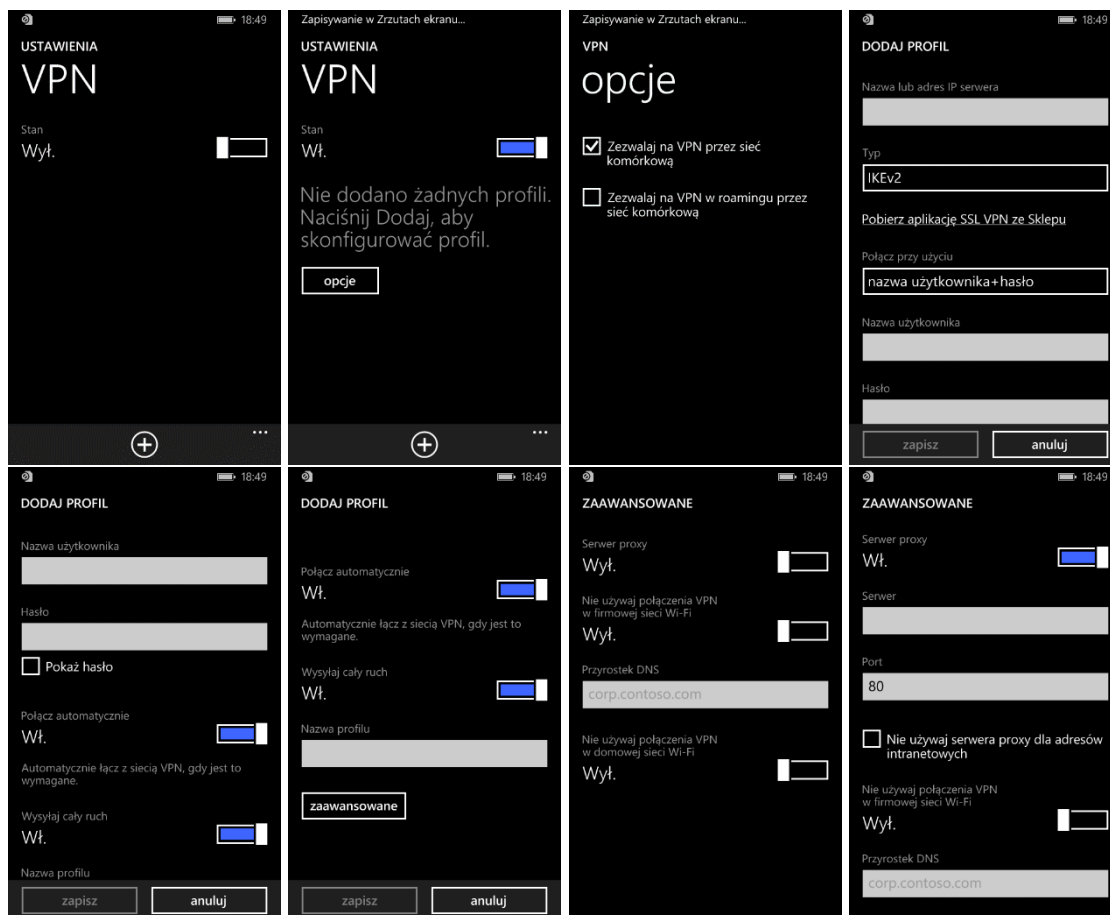
Ocena ryzyka

- Korzystając z funkcji **VPN** należy mieć na uwadze to, że mogą funkcjonować rozwiązania, których celem jest analizowanie i przechwytywanie ruchu a tym samym zdalne wpływanie na urządzenia, które korzystają z zestawionego połączenia.
- Włączenie opcji **VPN** zwiększa transfer danych.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Stan	Wł. Wył.	Wył.	Wył.
Zezwalaj na VPN przez sieć komórkową	Wł. Wył.	Wł.	Wł.
Zezwalaj na VPN w roamingu przez sieć komórkową	Wł. Wył.	Wył.	Wył.
Połącz przy użyciu	login + hasło certyfikat	-	certyfikat
Sprawdzanie certyfikatu serwera	Wł. Wył.	Wył.	Wł.
Połącz automatycznie	Wł. Wył.	Wł.	Wł.
Wysyłaj cały ruch	Wł. Wył. (domeny) Wył. (zakresy IP)	Wł.	
Serwer proxy	Wł. Wył.	Wył.	Wył.

Nie używaj połączenia VPN w firmowej sieci Wi-Fi	Wł. Wył.	Wył.	Wył.
Nie używaj połączenia VPN w domowej sieci Wi-Fi	Wł. Wył.	Wył.	Wył.



Rys. 23 Konfiguracja połączenia VPN

4.1.13 Kącik z aplikacjami

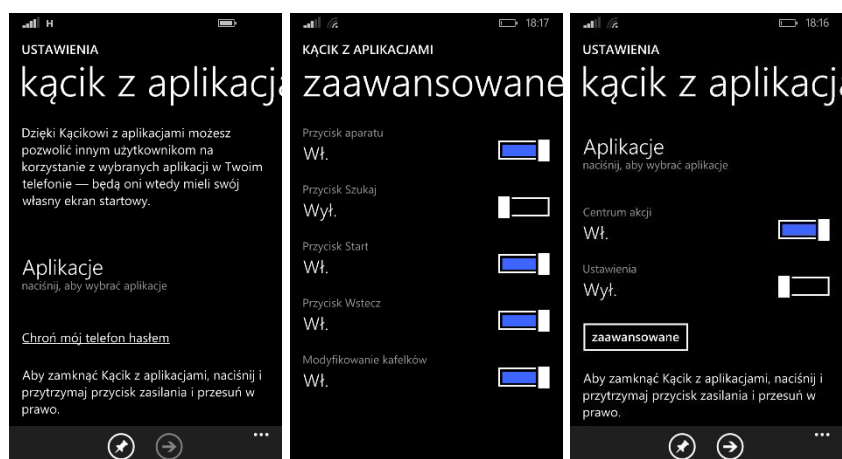
Kącik z aplikacjami umożliwia skonfigurowanie niestandardowego ekranu startowego telefonu Windows Phone 8.1, na którym będą znajdować się wyłącznie aplikacje udostępnione osobom korzystającym z telefonu. Ustawienia **Kącika z aplikacjami** można wyeksportować w celu zastosowania ich na innych urządzeniach co pozwala na standaryzację konfiguracji na urządzeniach współpracowników.

Ocena ryzyka

- Należy mieć na uwadze, że wykorzystywane funkcje w ramach wybranych aplikacji mogą wpływać na stan zabezpieczeń telefonu (np. wybór aplikacji Aparat umożliwia dostęp do biblioteki zdjęć, wybór aplikacji realizującej funkcje nawigacji GPS powoduje aktywację lokalizacji położenia).

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Centrum akcji	Wł. Wył.	Wł.	Wył.
Ustawienia	Wł. Wył.	Wył.	Wył.
Przycisk aparatu	Wł. Wył.	Wł.	Wył.
Przycisk Szukaj	Wł. Wył.	Wył.	Wył.
Przycisk Start	Wł. Wył.	Wł.	Wył.
Przycisk Wstecz	Wł. Wył.	Wł.	Wył.
Modyfikowanie kafelków	Wł. Wył.	Wł.	Wył.



Rys. 24 Kącik z aplikacjami

4.1.14 Praca

Firmy, organizacje, uniwersytety i inni pracodawcy mogą tworzyć na telefonie z systemem Windows Phone konto firmowe służące do dostarczania aplikacji i danych przydatnych w pracy. Konto firmowe może również służyć do wprowadzania zmian zwiększających bezpieczeństwo danych związanych z pracą. Skonfigurowanie konta firmowego może spowodować zainstalowanie w telefonie następujących elementów:

- nowe zasady zabezpieczeń,
- nowe aplikacje,
- nowe centrum.

Większość kont firmowych jest związana z pewną liczbą zasad, które mają zabezpieczyć telefon i znajdujące się w nim dane związane z pracą. Zasady mogą również dodawać lub usuwać funkcje wpływające na sposób działania telefonu z systemem Windows Phone. Firma może na przykład:

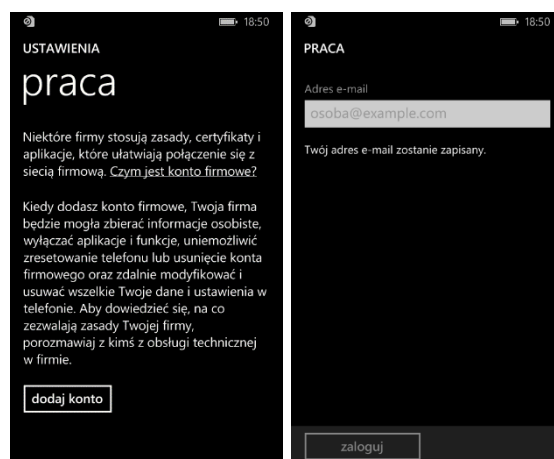
- wymagać hasła o określonej długości lub złożoności (może to wymagać zmiany dotychczasowego hasła),
- wyłączyć kartę pamięci (jeśli jest w telefonie),
- zdalnie zresetować telefon do oryginalnego stanu fabrycznego,
- wyłączyć wbudowane aplikacje, np. Internet Explorer,
- uniemożliwić działanie określonych aplikacji zainstalowanych w telefonie,
- uniemożliwić pobieranie określonych aplikacji ze Sklepu Windows Phone,
- uniemożliwić usunięcie konta firmowego.

Ocena ryzyka

- Wykorzystywanie opcji **Praca** umożliwia dostęp do aplikacji oraz danych przedsiębiorstwa dostępnych dla użytkowników mobilnych.

Minimalizacja ryzyka

Wykorzystywanie opcji **Praca** otwiera możliwości w zakresie centralnego zarządzania ustawieniami urządzeń z Windows Phone. Tym samym minimalizacja ryzyka jest możliwa poprzez odpowiedni dobór zasad zabezpieczeń w środowisku Windows Intune lub System Center Configuration Manager.



Rys. 25 Ustawienie opcji **Praca**

4.1.15 Kącik dziecięcy

Opcja **Kącik dziecięcy** pozwala korzystać z dodanych przez właściciela telefonu gier, aplikacji, muzyki i wideo ale uniemożliwia przejście do wszystkich pozostałych danych zgromadzonych na telefonie.

Ocena ryzyka

- Konfiguracja dostępu do określonych aplikacji może nieść ze sobą pośrednio dostęp do zgromadzonych przez oprogramowanie danych (np. aplikacja Aparat daje dostęp do biblioteki zdjęć).
- Włączenie funkcji bez hasła ekranu blokady daje pełny dostęp do urządzenia.

Minimalizacja ryzyka

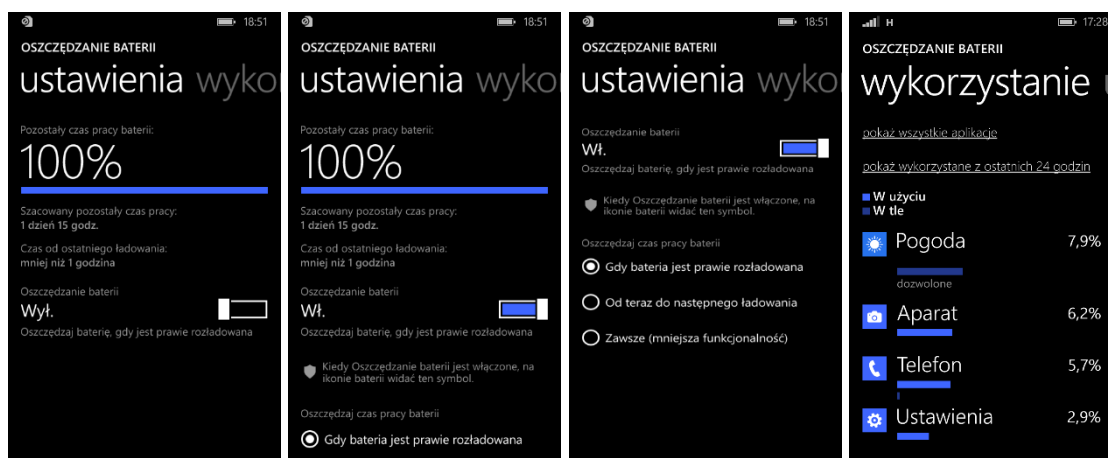
Zaleca się stosowanie hasła ekranu blokady zgodnie z wytycznymi w punkcie 4.1.4.



Rys. 26 Ustawienie opcji *Kącik dziecięcy*

4.1.16 Oszczędzanie baterii

W ramach sekcji można wyłączyć niepotrzebne funkcje i zapewnić oszczędzanie baterii. Dodatkowo można także uzyskać informacje o wykorzystaniu baterii przez poszczególne aplikacje.



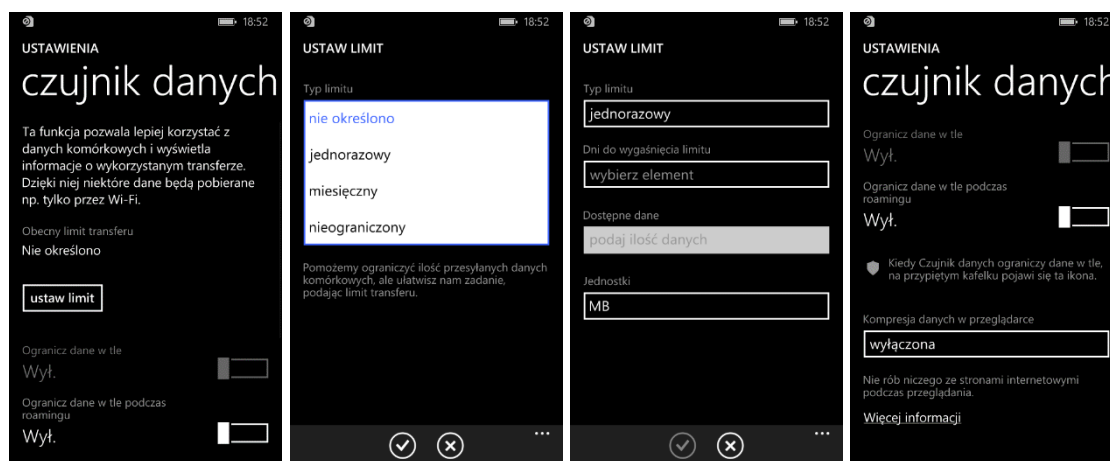
Rys. 27 Opcje ustawień *Oszczędzanie baterii*

Ocena ryzyka

Wybór ustawień w ramach **Oszczędzanie baterii** nie ma wpływu na opcje zabezpieczeń urządzenia gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.17 Czujnik danych

Czujnik danych pokazuje szczegółowy podział wykorzystania danych w telefonie Windows Phone i pomaga uniknąć nieoczekiwanych opłat, ponieważ ostrzega o zbliżaniu się do limitu planu taryfowego. Dodatkową zaletą jest możliwość odkładania zadań z dużą transmisją danych na czas podłączenia do sieci Wi-Fi.



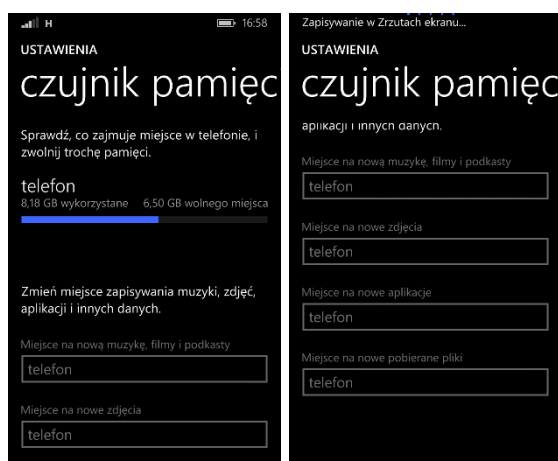
Rys. 28 Opcje ustawień **Czujnik danych**

Ocena ryzyka

Wybór ustawień w ramach **Czujnik danych** nie ma wpływu na opcje zabezpieczeń urządzenia gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.18 Czujnik pamięci

Czujnik pamięci umożliwia sprawdzanie wolnej pamięci oraz zmianę miejsca zapisywania muzyki, zdjęć, aplikacji i innych danych. Dodatkowo można z tego poziomu usuwać pliki tymczasowe.



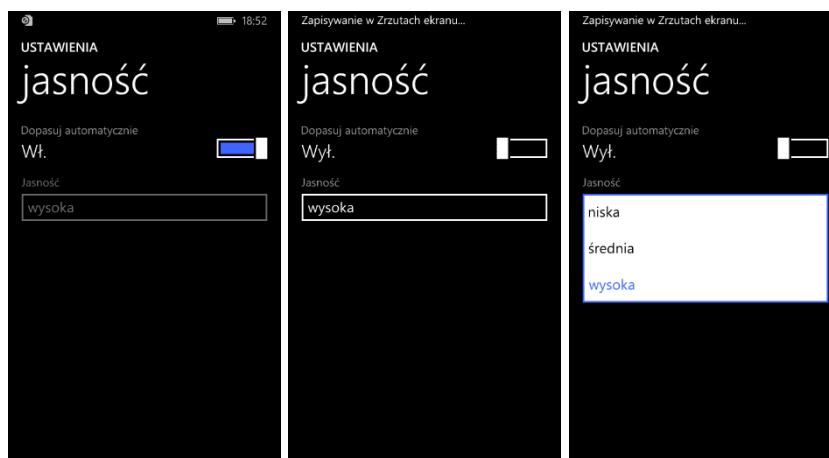
Rys. 29 Opcje ustawień **Czujnik pamięci**

Ocena ryzyka

Sekcja **Czujnik pamięci** stanowi źródło informacji z możliwością odinstalowania aplikacji oraz usunięcia plików tymczasowych więc nie ma wpływu na opcje zabezpieczeń urządzenia.

4.1.19 Jasność

Opcje sekcji umożliwiają określenie ustawień jasności ekranu.



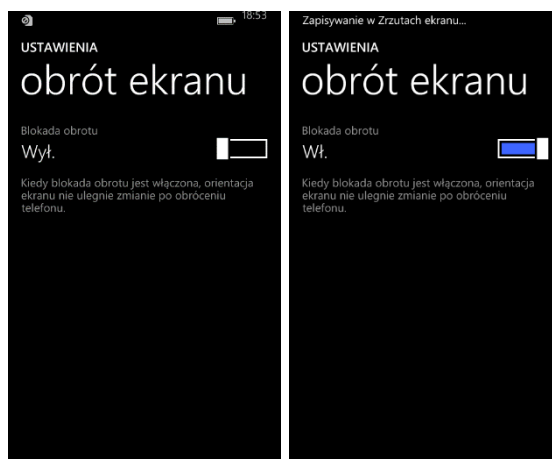
Rys. 30 Opcje ustawień *Jasność*

Ocena ryzyka

Wybór ustawień w ramach **Jasność** nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.20 Obrót ekranu

Opcja umożliwia włączenie blokady obrotu ekranu, która powoduje że w przypadku obrócenia telefonu nie ulegnie zmianie orientacja telefonu.



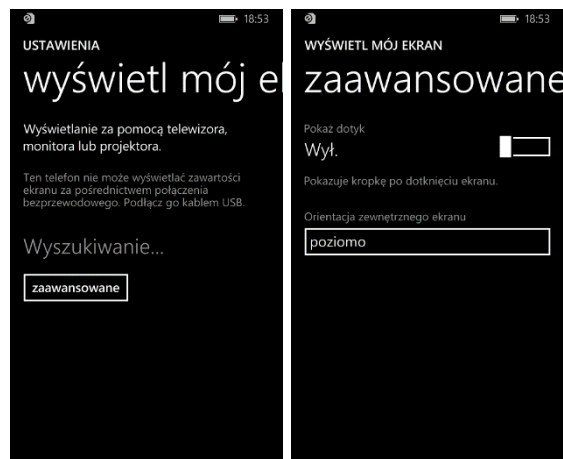
Rys. 31 Opcje ustawień *Obrót ekranu*

Ocena ryzyka

Wybór ustawień w ramach **Obrót ekranu** nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.21 Wyświetl mój ekran

Sekcja umożliwia konfigurację i wyświetlanie ekranu na zewnętrznym monitorze lub rzutniku.



Rys. 32 Opcje ustawień *Wyświetl mój ekran*

Ocena ryzyka

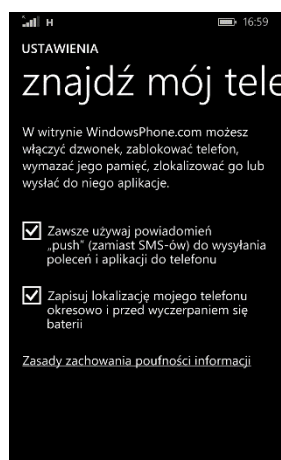
- W przypadku korzystania z opcji należy pamiętać, że wyświetlanie ekranu telefonu może spowodować zapoznanie się nieuprawnionych osób z przechowywanymi w urządzeniu informacjami.
- Wpisywane znaki haseł w trakcie wyświetlania ekranu są oznaczane/podświetlane co umożliwia ich poznanie.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Pokaż dotyk	Wł. Wył.	Wł.	Wył.

4.1.22 Znajdź mój telefon

Opcja umożliwia konfigurację opcji pozwalających na lokalizację telefonu. Po włączeniu można zablokować telefon, wymazać go, włączyć jego dzwonek lub sprawdzić położenie telefonu na mapie przy użyciu dowolnego komputera podłączonego do Internetu. Do działania jest wymagane konto Microsoft.



Rys. 33 Opcje ustawień *Znajdź mój telefon*

Ocena ryzyka

- Włączenie opcji **Zapisuj lokalizację mojego telefonu okresowo i przed wyczerpaniem się baterii** wiąże się z wykorzystywaniem opcji lokalizacji. Włączenie funkcji lokalizacji zwiększa transfer danych oraz powoduje, że dane osobiste są wysyłane z urządzenia do źródeł korzystających z omawianych opcji.
- Nie korzystanie z opcji **Zawsze używaj powiadomień „push” (zamiast SMS-ów) do wysyłania poleceń i aplikacji do telefonu** powoduje, że powiadomienia będą działać wolniej a także będzie stosowało się ograniczenie do 15 wiadomości SMS w czasie trzech dni co może uniemożliwić skorzystanie z funkcji Znajdź mój telefon.

Minimalizacja ryzyka

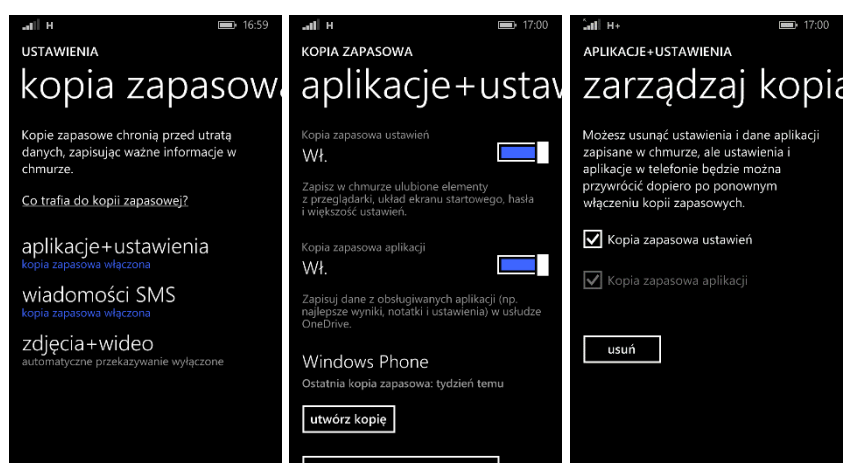
Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Zapisuj lokalizację mojego telefonu okresowo i przed wyczerpaniem się baterii	Wł. Wył.	Wył.	Wł.
Zawsze używaj powiadomień „push” (zamiast SMS-ów) do wysyłania poleceń i aplikacji do telefonu	Wł. Wył.	Wył.	Wł.

4.1.23 Kopia zapasowa

W ramach sekcji można zarządzać oraz skonfigurować opcje kopii zapasowych:

- aplikacji i ustawień,
- wiadomości SMS,
- zdjęć i wideo.

Do działania jest wymagane konto Microsoft.



Rys. 34 Opcje ustawień Kopia zapasowa

Ocena ryzyka

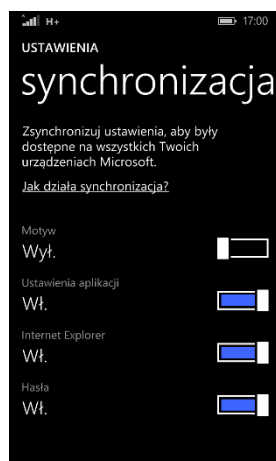
- Brak kopii zapasowych prowadzi do utraty danych w przypadku awarii urządzenia lub jego zagubienia.
- Dostęp do plików kopii zapasowej przez nieuprawnionych użytkowników jest równoznaczny z uzyskaniem chronionych danych.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Kopia zapasowa ustawień	Wł. Wył.	Wł.	Wł.
Kopia zapasowa aplikacji	Wł. Wył.	Wł.	Wł.
Kopia zapasowa SMS-ów	Wł. Wył.	Wył.	Wł.
Zdjęcia	Nie przekazuj Dobra jakość (możliwy transfer danych) Najlepsza jakość (wymaga Wi-Fi)	Dobra jakość (możliwy transfer danych)	Dobra jakość (możliwy transfer danych)
Filmy	Nie przekazuj Najlepsza jakość (wymaga Wi-Fi)	Nie przekazuj	Nie przekazuj

4.1.24 Synchronizacja ustawień

Opcje sekcji umożliwiają konfigurację ustawień aby były dostępne na wszystkich wykorzystywanych przez użytkownika urządzeniach Microsoft.



Rys. 35 Opcje ustawień *Synchronizacja ustawień*

Ocena ryzyka

- Korzystanie z opcji wiąże się z synchronizacją motywu, ustawień aplikacji, ustawień Internet Explorer oraz haseł na innych urządzeniach. W przypadku nieuprawnionego do nich dostępu stanowi to potencjalne źródło wycieku informacji poufnych oraz osobistych użytkownika.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Motyw	Wł. Wył.	Wł.	Wł.
Ustawienia aplikacji	Wł. Wył.	Wł.	Wł.
Internet Explorer	Wł. Wył.	Wł.	Wł.
Hasła	Wł. Wył.	Wł.	Wył.

4.1.25 Tryb samochodowy

Tryb samochodowy powoduje wyłączenie na czas kierowania samochodem wszystkich powiadomień oprócz SMS-ów i połączeń telefonicznych. Istnieje także możliwość wyłączenia powiadomień SMS i połączeń telefonicznych. Do skorzystania z funkcji niezbędne jest urządzenie Bluetooth.



Rys. 36 Opcje ustawień *Tryb samochodowy*

Ocena ryzyka

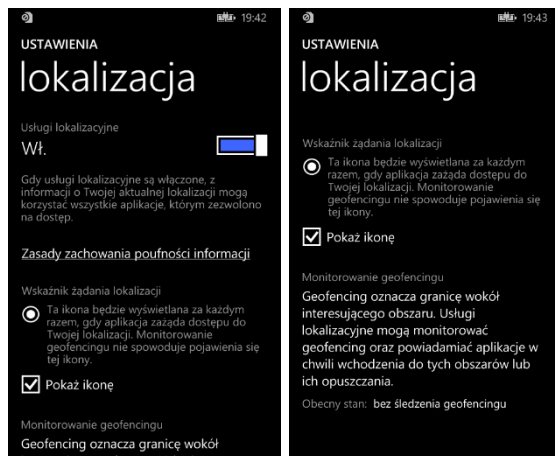
- Wybór ustawień w ramach **Tryb samochodowy** nie ma wpływu na opcje zabezpieczeń urządzenia gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.
- Wybór ustawień w ramach **Tryb samochodowy** ma wpływ na bezpieczeństwo w ruchu komunikacyjnym.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Ignoruj połączenia	Wł. Wył.	Wył.	Wył.
Ignoruj SMS-y	Wł. Wył.	Wył.	Wł.

4.1.26 Lokalizacja

Sekcja umożliwia włączenie lokalizacji, która przekazywana jest aplikacjom, którym zezwolono na dostęp. Ponadto istnieje możliwość konfiguracji geofencingu, który odpowiada za wykrywanie granic wokół interesującego obszaru.



Rys. 37 Opcje ustawień **Lokalizacja**

Ocena ryzyka

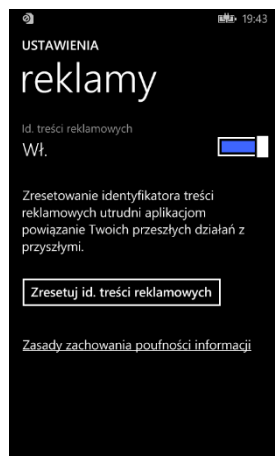
- Włączenie funkcji zwiększa transfer danych oraz powoduje, że dane osobiste są wysyłane z urządzenia do źródeł korzystających z omawianych opcji.
- Korzystanie z lokalizacji powoduje, że dane są dostępne dla operatora komórkowego.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Usługi lokalizacyjne	Wł. Wył.	Wł.	Wł.

4.1.27 Id. treści reklamowych

Sekcja umożliwia konfigurację identyfikatorów treści reklamowych. W celu lepszego dostosowania reklam, system Windows Phone umożliwia aplikacjom uzyskiwanie dostępu do identyfikatora unikalnego dla każdej osoby korzystającej z telefonu z systemem Windows Phone. Dostęp do tego identyfikatora można w każdej chwili zresetować lub wyłączyć. Jeśli zostało wybrane zezwolenie aplikacjom na uzyskiwanie dostępu do identyfikatora treści reklamowych, system Windows Phone udostępni go wszystkim aplikacjom, które go zażądataj. Aplikacje mogą przechowywać lub przysyłać te informacje. Twórcy aplikacji i sieci reklamowe korzystają z identyfikatora treści reklamowych w celu dostarczania interesujących reklam na podstawie analizy używanych przez użytkownika aplikacji. Twórcy aplikacji mogą go również używać do ulepszania jakości usług, ponieważ identyfikator ten umożliwia im określanie częstotliwości i skuteczności reklam oraz wykrywanie oszustw i zagrożeń dla bezpieczeństwa telefonu. Jeśli zostanie włączony dostęp do identyfikatora treści reklamowych, każde skorzystanie z niego przez daną aplikację będzie zgodne z obowiązującymi w jej przypadku zasadami ochrony prywatności. Po wyłączeniu tego ustawienia do aplikacji żądających dostępu do identyfikatora treści reklamowych nie będą wysyłane żadne informacje. Po ponownym włączeniu ustawienia generowany jest nowy identyfikator.



Rys. 38 Opcje ustawień **Reklamy**

Ocena ryzyka

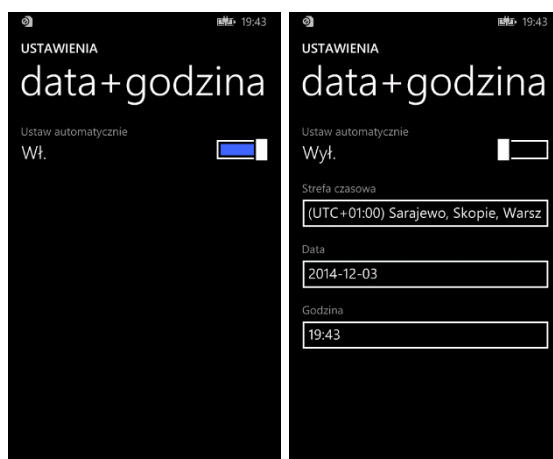
- Korzystanie z opcji powoduje wyświetlanie spersonalizowanych reklam dla użytkownika na podstawie wykonywanych przez niego działań w urządzeniu.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Id. treści reklamowych	Wł. Wył.	Wył.	Wył.

4.1.28 Data + godzina

Sekcja umożliwia ręczną lub automatyczną konfigurację daty, godziny oraz strefy czasowej.



Rys. 39 Opcje ustawień **Data + godzina**

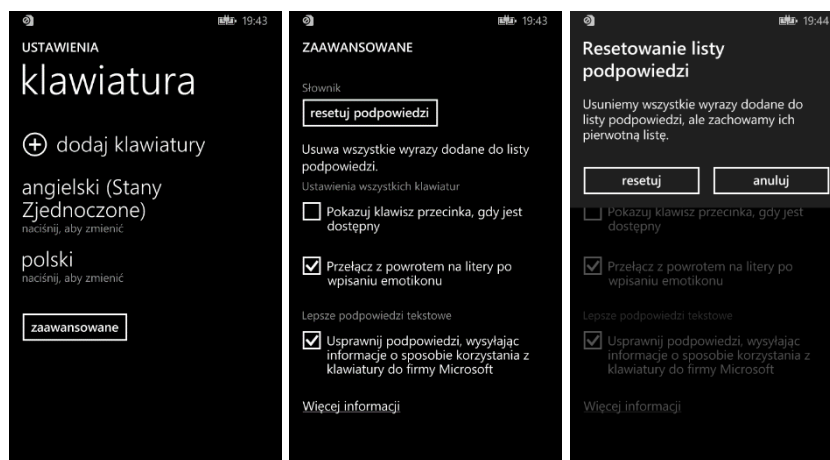
Ocena ryzyka

Wybór ustawień w ramach **Data + godzina** nie ma wpływu na opcje zabezpieczeń urządzenia gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.29 Klawiatura

Sekcja umożliwia konfigurację języków klawiatury oraz dodatkowych opcji związanych z jej obsługą (np. podpowiadanie tekstów, wstawianie spacji, rozpoczynanie zdań wielką literą itp.)

Podczas pisania system Windows Phone może podpowiadać słowa i poprawki na podstawie zawartości słownika telefonu. W miarę upływu czasu telefon automatycznie dostosowuje się, aby podpowiadać słowa, które zostały wcześniej napisane (na przykład nazwiska). Te słowa są przechowywane tylko w telefonie. Telefon może również podpowiadać słowa na podstawie ostatnich wątków wiadomości. W większości języków można wybrać wyłączenie tych podpowiedzi. Decydując się na uczestnictwo w programie wysyłania informacji dotyczących klawiatury dotykowej mamy wpływ na usprawnianie funkcji pisania w telefonie Windows Phone, a także ulepszanie innych produktów i usług firmy Microsoft. Po włączeniu tej funkcji informacje o korzystaniu z klawiatury dotykowej używane przez system Windows Phone do rozpoznawania wpisywanych znaków („punkty dotyku”) są przesyłane do firmy Microsoft w przypadku każdego użycia klawiatury w telefonie. Wszystkie wpisane znaki, wyrazy wybrane spośród podpowiedzi i automatyczne korekty również zostaną przesłane. Ponieważ znajomość wyrazów wpisywanych przez użytkowników w telefonach zwiększa trafność interpretowania wpisywanych znaków, wysyłany będzie również tekst. W celu ochrony prywatności użytkownika nie są gromadzone informacje dotyczące klawiatury dotykowej, gdy w telefonie wyświetlany jest ekran logowania lub pole hasła. Stosowane są również środki mające na celu uniemożliwienie zbierania adresów e-mail i sekwencji cyfr, takich jak numery telefonów czy numery kart kredytowych. Informacje dotyczące klawiatury są wysyłane z losowym identyfikatorem, który nie umożliwia identyfikacji telefonu. Następnie są łączone z tekstami uzyskanymi od wielu użytkowników systemu Windows Phone i przekształcane w sekwencje znaków i słów służące do analizy.



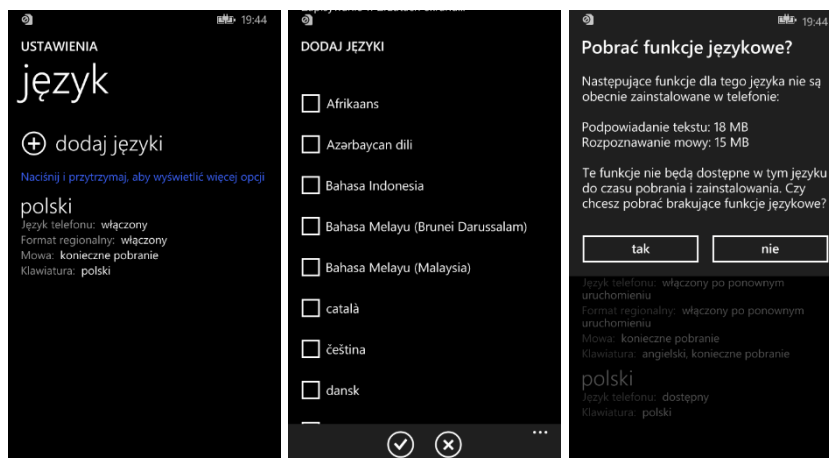
Rys. 40 Opcje ustawień **Klawiatura**

Ocena ryzyka

Wybór ustawień w ramach **Klawiatura** nie ma wpływu na opcje zabezpieczeń urządzenia gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.30 Język

Sekcja umożliwia dodanie języków i konfigurację opcji klawiatury, regionu i mowy.



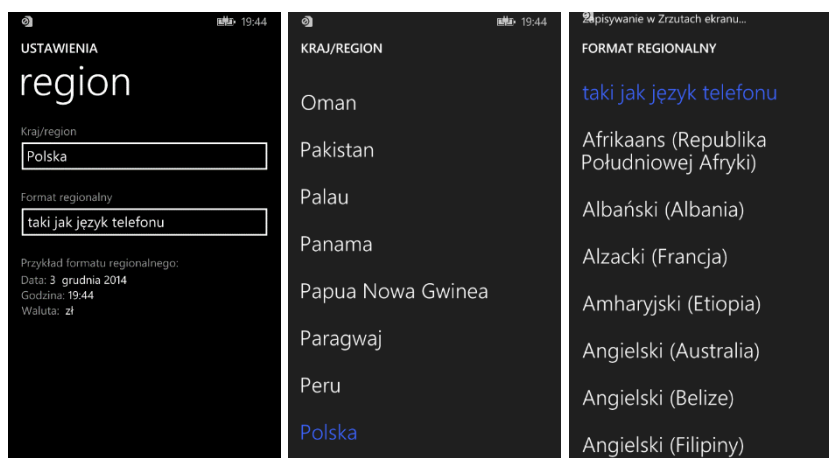
Rys. 41 Opcje ustawień *Język*

Ocena ryzyka

Wybór ustawień bezpośrednio w ramach sekcji Język nie ma wpływu na opcje zabezpieczeń urządzenia gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.31 Region

Ustawienia sekcji umożliwiają konfigurację kraju oraz formatu regionalnego.



Rys. 42 Opcje ustawień *Region*

Ocena ryzyka

Wybór ustawień w ramach sekcji **Region** nie ma wpływu na opcje zabezpieczeń urządzenia gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.32 Raport

Ustawienia sekcji odpowiadają za konfigurację wysyłania raportów o korzystaniu z telefonu w celu ulepszania produktów i usługi firmy Microsoft oraz jej partnerów.

Uczestnictwo w programie przesyłania raportów o działaniu systemu Windows Phone ma na celu pomoc firmie Microsoft w doskonaleniu tego systemu oraz innych produktów i usług. Decydując się na uczestnictwo w programie zbierane są podstawowe informacje o sposobie korzystania z telefonu, aplikacji oraz generowanych błędach w obszarach:

- Konfiguracja telefonu, np. używane połączenia sieciowe, rozdzielczość ekranu, użycie pamięci, czas pracy baterii, ustawienia domeny skonfigurowanych kont e-mail oraz wersja zainstalowanego systemu Windows Phone.
- Wydajność i niezawodność, np. informacje na temat tego, jak szybko dana funkcja odpowiada na naciśnięcie przycisku, ile występuje problemów związanych z daną funkcją oraz jak szybko informacje są wysyłane lub odbierane za pośrednictwem połączenia sieciowego.
- Korzystanie z aplikacji, np. najczęściej używane opcje, funkcje przypięte do ekranu startowego, sposób nawigowania w menu i Sklepie, częstość modyfikowania ustawień, pobierania aktualności oraz aktualizowania informacji kontaktowych, a także czas korzystania z określonych funkcji.
- Błędy w działaniu oprogramowania, np. problemy przeszkadzające w korzystaniu z telefonu oraz błędy występujące w sposób niewidoczny dla użytkownika. Raporty mogą zawierać informacje osobiste, ale firma Microsoft używa ich do diagnozowania błędów, a nie do identyfikowania użytkownika ani do kontaktowania się z nim. Na przykład raport zawierający migawkę pamięci urządzenia może zawierać fragment otwartej wiadomości e-mail lub SMS albo dane przesłane ostatnio do witryny internetowej.
- Raporty dobrowolnie przesyłane do firmy Microsoft.
Firma Microsoft nie używa informacji zebranych w raportach do identyfikowania użytkowników, chyba że użytkownik jawnie zezwoli na to w przypadku określonej funkcji (np. w celu wyświetlania propozycji w Sklepie). Firma Microsoft używa tych informacji, aby usprawnić najczęściej używane produkty i funkcje oraz opracować rozwiązania często występujących problemów. Zbierane informacje, a w szczególności raporty dotyczące błędów, mogą zawierać dane osobowe, ale firma Microsoft używa tych informacji do diagnozowania błędów, a nie do identyfikowania użytkownika ani do kontaktowania się z nim. W celu doskonalenia produktów i usług działających na podstawie oprogramowania firmy Microsoft może ona udostępniać informacje z programu raportów twórcom sprzętu i innym zaufanym partnerom. Zabraniaamy tym partnerom wykorzystania tych informacji w celu identyfikowania użytkowników lub kontaktowania się z nimi.
- Automatyczne aktualizacje telefonu
Firma Microsoft publikuje aktualizacje systemu operacyjnego telefonu zawierające przydatne lub krytyczne usprawnienia. Aby użytkownik mógł na bieżąco otrzymywać informacje o nowych aktualizacjach, telefon regularnie sprawdza ich dostępność. Po włączeniu tej opcji aktualizacje są pobierane automatycznie. Użytkownik będzie nadal powiadamiany o pobranych aktualizacjach i proszony o ich instalację. Aktualizacje krytyczne będą instalowane automatycznie. Po wyłączeniu tej opcji użytkownik będzie powiadamiany o dostępnych aktualizacjach do pobrania i będzie mógł zdecydować, kiedy mają zostać pobrane i zainstalowane.
- Uzyskiwanie automatycznych aktualizacji aplikacji ze Sklepu

Twórcy aplikacji często wykonują ich aktualizacje. W zależności od liczby zainstalowanych aplikacji w telefonie liczba aktualizacji będzie zróżnicowana. Aby ułatwić pobieranie aktualizacji (w zależności od ustawień transmisji danych przez sieć komórkową), można wybrać opcję automatycznego pobierania aktualizacji.



Rys. 43 Opcje ustawień *Raport*

Ocena ryzyka

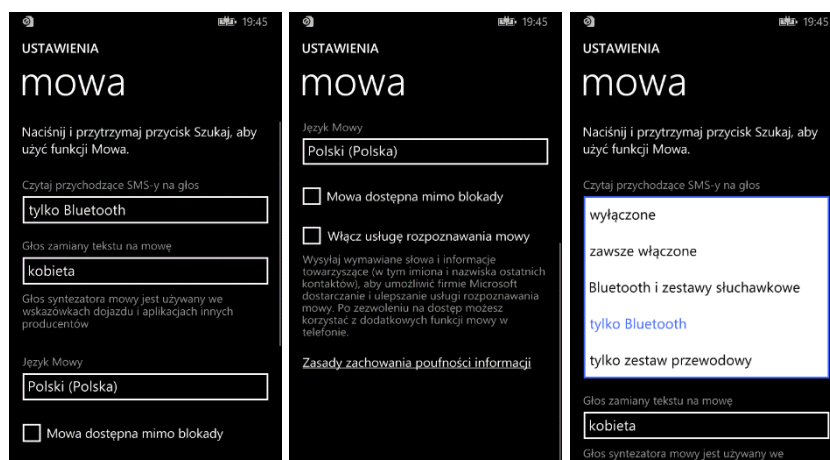
- Korzystanie z opcji powoduje przesyłanie raportów o korzystaniu z telefonu co może powodować, że dane osobiste będą wysyłane z urządzenia do źródeł korzystających z omawianych opcji.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Wysyłaj raporty	Wł. Wył.	Wł.	Wył.

4.1.33 Mowa

Sekcja umożliwia konfigurację funkcji, która pozwala na czytanie przychodzących wiadomości SMS.



Rys. 44 Opcje ustawień *Mowa*

Ocena ryzyka

- W przypadku korzystania z funkcji **Mowa** istnieje ryzyko zapoznania się przez osoby niepowołane z treścią wiadomości SMS kierowanych do użytkownika telefonu.

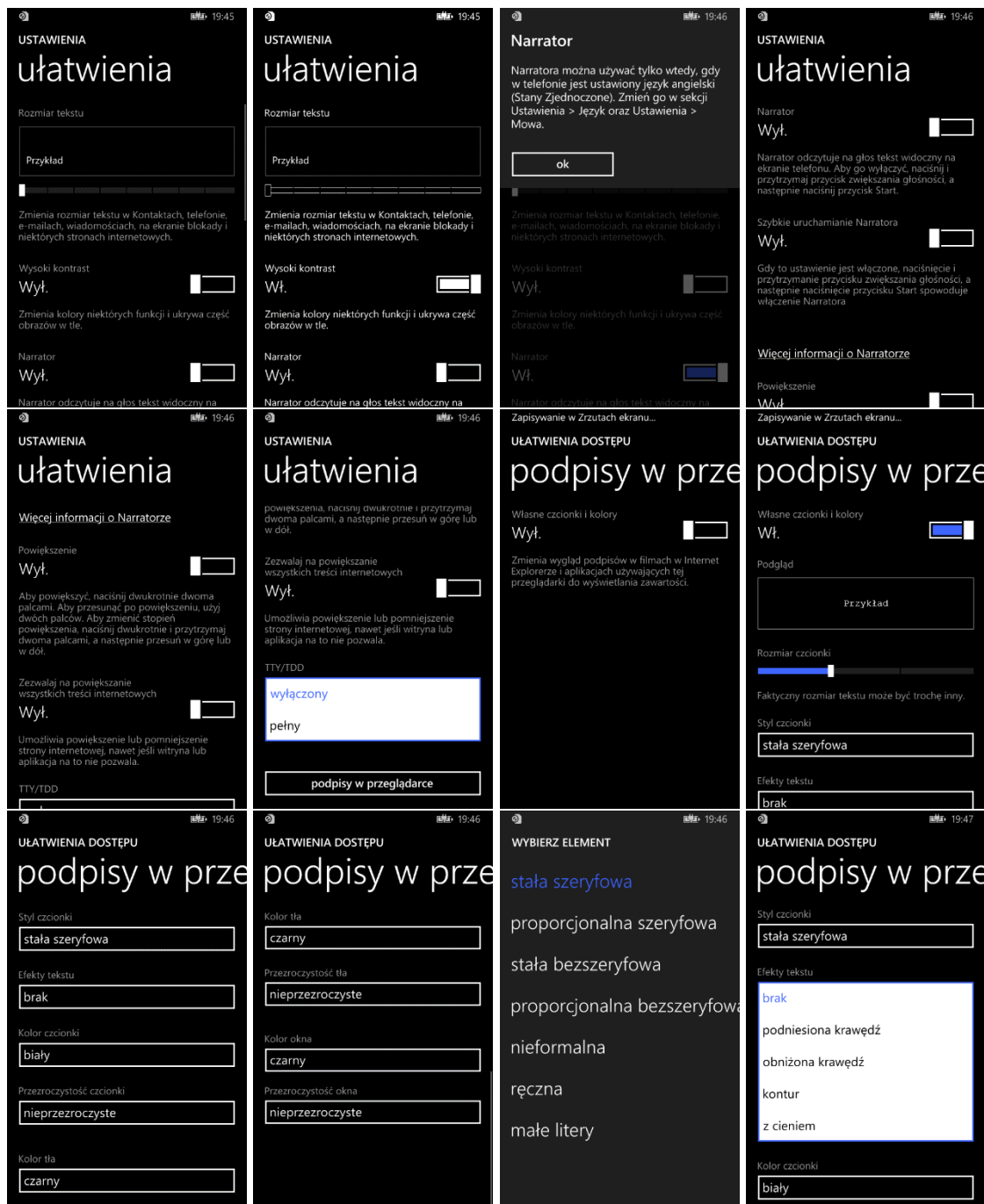
Minimalizacja ryzyka

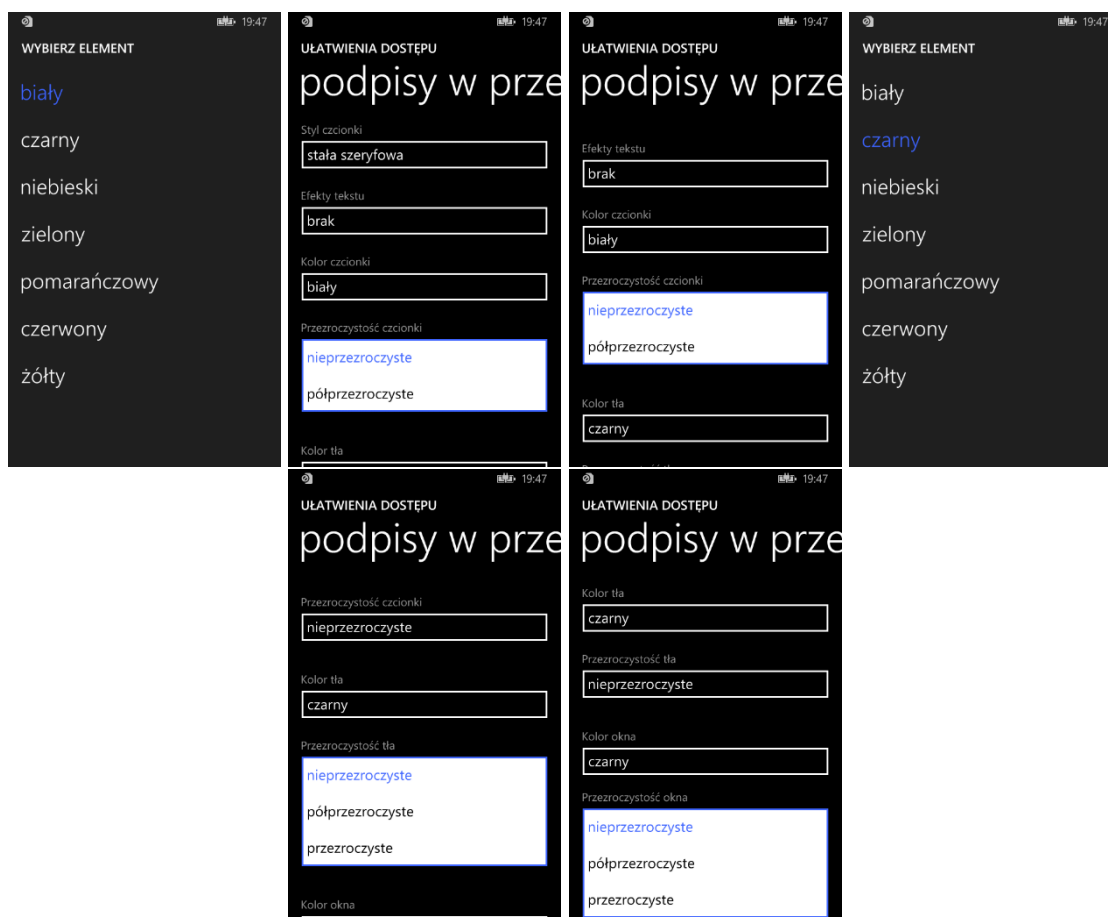
Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Czytaj przychodzące SMS-y na głos	wyłączone zawsze włączone Bluetooth i zestawy słuchawkowe tylko Bluetooth tylko zestaw przewodowy	Bluetooth i zestawy słuchawkowe	wyłączone
Mowa dostępna mimo blokady	Wł. Wył.	Wył.	Wył.

4.1.34 Ułatwienia dostępu

Ułatwienia dostępu umożliwiają określenie:

- rozmiaru tekstu,
- konfigurację wysokiego kontrastu,
- wykorzystanie funkcji Narrator i sposobu jej włączenia,
- ustawień powiększania,
- konfigurację treści internetowych,
- konfigurację trybu TTY/TDD,
- podpisów w przeglądarce na które składają się ustawienia wyglądu przeglądarki.





Rys. 45 Opcje ustawień *Ułatwienia dostępu*

Ocena ryzyka

Wybór ustawień w ramach sekcji **Ułatwienia dostępu** z uwagi na ich przeznaczenie nie podlega ocenie ryzyka w zakresie zabezpieczeń urządzenia.

4.1.35 Aplikacje dla akcesoriów

W ramach sekcji istnieje możliwość konfiguracji telefonu z takimi urządzeniami jak inteligentne zegarki, inteligentne obudowy telefonów, czujniki fitness i budziki.

Niektóre akcesoria mogą pobierać powiadomienia z telefonu takie jak:

- informacje o nadchodzących połączeniach telefonicznych włącznie z identyfikatorem osoby dzwoniącej,
- wiadomości SMS, w tym informacje o nadawcy i treść wiadomości,
- przypomnienia,
- alarmy,
- banery powiadomień pochodzących od innych firm,
- wiadomości e-mail,
- metadane odtwarzania multimediów.



Rys. 46 Opcje ustawień *Aplikacje dla akcesoriów*

Ocena ryzyka

- Korzystanie z funkcji **Aplikacje dla akcesoriów** może stanowić źródło dostępu do danych poufnych użytkownika jeśli osoba postronna ma dostęp do podłączonego akcesoria.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Aplikacja dołączona do akcesoria	Zależne od aplikacji	Zależne od aplikacji	Zależne od aplikacji

4.1.36 Aktualizacje

W ramach sekcji można sprawdzić dostępność aktualizacji oraz uruchomić proces aktualizacji urządzenia. Dodatkowo istnieje możliwość konfiguracji automatycznego pobierania w odniesieniu do ustawień transmisji danych.



Rys. 47 Opcje ustawień *Aktualizacje*

Ocena ryzyka

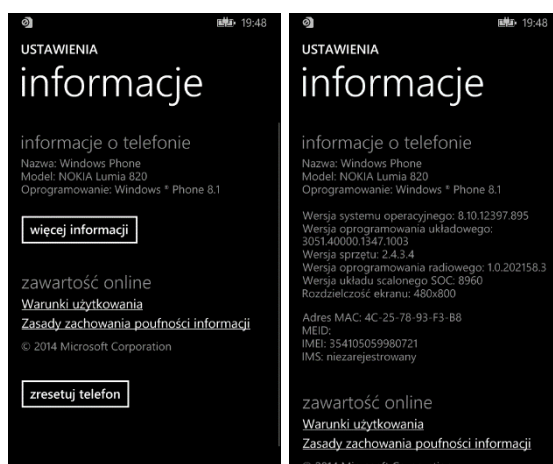
- Brak polityki aktualizacji urządzeń lub niedbanie o ich instalację naraża użytkownika urządzenia na działanie znanych podatności związanych z omijaniem zabezpieczeń.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Automatycznie pobieraj aktualizacje, jeśli zezwalają na to ustawienia transmisji danych	Wł. Wył.	Wł.	Wł.

4.1.37 Informacje

Sekcja umożliwia uzyskanie szczegółowych informacji na temat urządzenia, systemu operacyjnego, warunków użytkowania czy zasad zachowania poufności informacji. Dodatkowo istnieje możliwość wykonania z tego poziomu resetu telefonu do ustawień fabrycznych co powoduje wymazanie całej zawartości osobistej, w tym aplikacji, gier, zdjęć, muzyki i filmów.



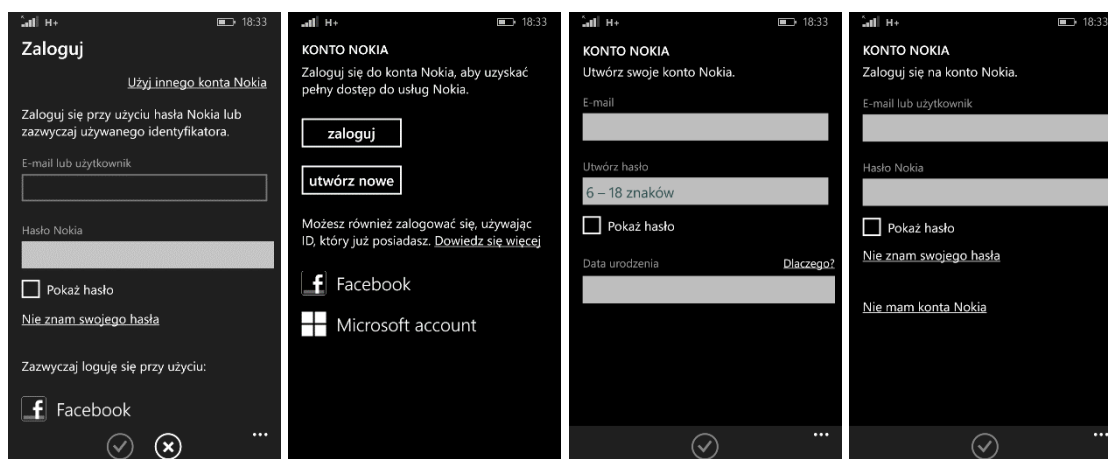
Rys. 48 Opcje ustawień **Informacje**

Ocena ryzyka

W przypadku niepowołanego dostępu do opcji resetowania urządzenia istnieje ryzyko utraty danych, które nie zostały zarchiwizowane.

4.1.38 Konto Nokia

Konto Nokia zapewnia pełny dostęp do usług Nokia i pomaga zarządzać kontem użytkownika, jego danymi oraz sposobem komunikacji z serwisem Nokia.



Rys. 49 Opcje ustawień **Konto Nokia**

Ocena ryzyka

- Korzystanie z konta Nokia powoduje przesyłanie informacji i danych użytkownika do źródeł odpowiedzialnych za działanie usługi.
- Działanie funkcji wymaga zezwolenia na dostęp do imienia i nazwiska, płci, awataru, kontaktów i znajomych użytkownika telefonu.
- Korzystanie z konta Nokia narzuca automatyczne logowanie oraz dostęp do adresów e-mail użytkownika urządzenia.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Konto Nokia	Wł. Wył.	Wył.	Wył.

4.1.39 Punkt dostępu

Konfiguracja punktu dostępu umożliwia łączność z siecią Internet oraz wysyłanie wiadomości multimedialnych (MMS).

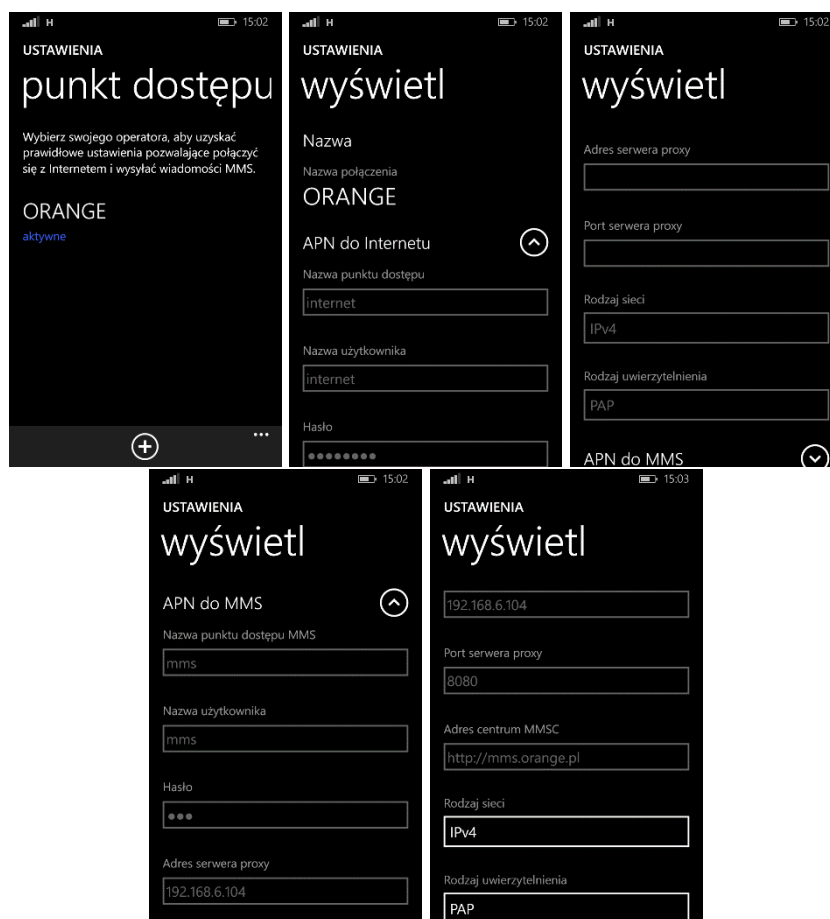
Wykonując w telefonie czynności wymagające połączenia sieciowego (np. wysyłanie wiadomości e-mail, pobieranie aktualności z sieci społecznościowych, przeglądanie witryn sieci Web, pobieranie aplikacji) urządzenie automatycznie łączy się z siecią komórkową w celu przesłania informacji. Jeśli telefon ma połączenie z siecią Wi-Fi jest ona używana zamiast połączenia komórkowego.

Ocena ryzyka

- Posiadanie skonfigurowanego i aktywnego punktu dostępu, umożliwia urządzeniu i zainstalowanym na nim aplikacjom na korzystanie w tle z transmisji danych.
- Włączenie funkcji zwiększa transfer danych oraz powoduje, że dane osobiste są wysyłane z urządzenia do źródeł korzystających z omawianych opcji.

Minimalizacja ryzyka

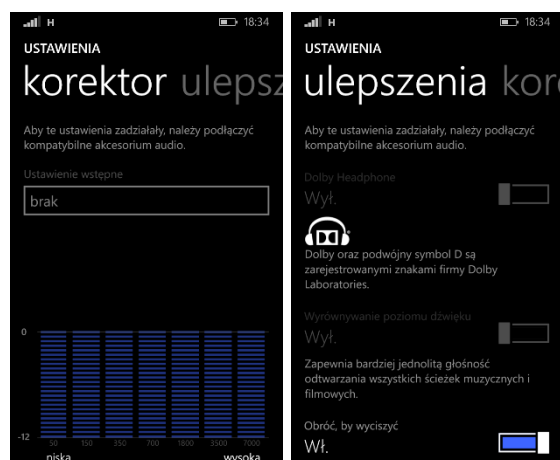
Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Punkt dostępu	Wł. Wył.	Wł.	Wł.



Rys. 50 Opcje ustawień **Punkt dostępu**

4.1.40 Audio

Ustawienia w sekcji umożliwiają konfigurację korekcji dźwięku oraz dodatkowe opcje związane z odtwarzaniem muzyki.



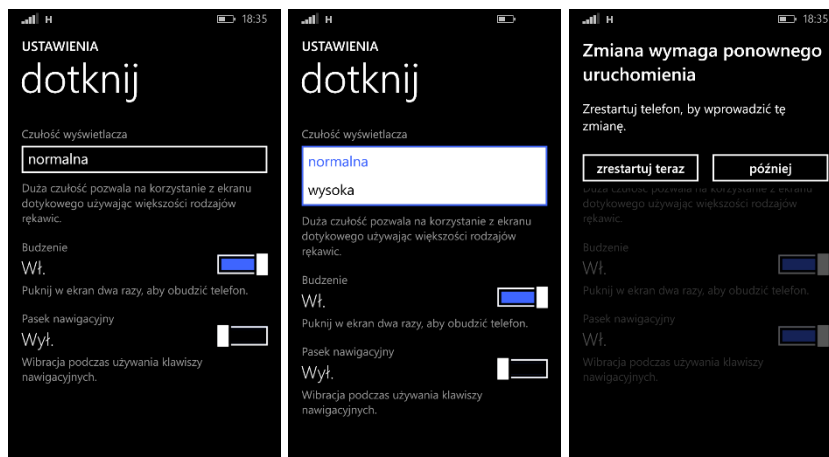
Rys. 51 Opcje ustawień **Audio**

Ocena ryzyka

Wybór ustawień w ramach **Audio** nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.41 Dotknij

Ustawienia w sekcji umożliwiają określenie czułości wyświetlacza na dotyk, włączenie opcji budzenia wyświetlacza po dwukrotnym jego naciśnięciu oraz określenie wibracji w trakcie używania klawiszy funkcyjnych.



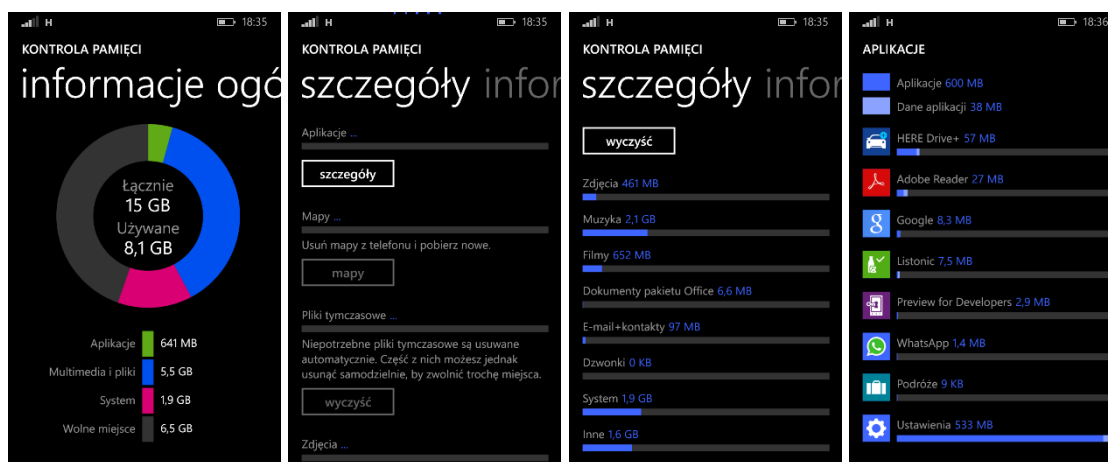
Rys. 52 Opcje ustawień *Dotknij*

Ocena ryzyka

Wybór ustawień w ramach **Dotknij** nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.42 Kontrola pamięci

W ramach sekcji prezentowana jest zawartość pamięci urządzenia oraz istnieje możliwość sprawdzenia wolnego i zajętego miejsca z opcją kasowania aplikacji, map czy plików tymczasowych.



Rys. 53 Opcje ustawień *Kontrola pamięci*

Ocena ryzyka

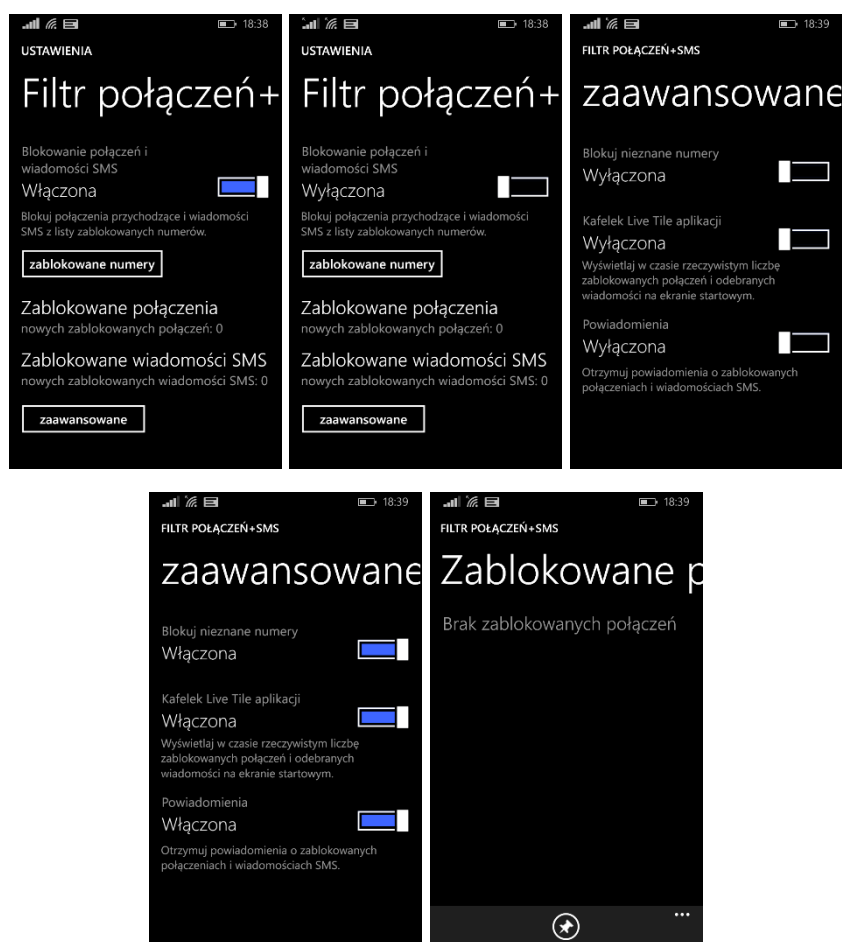
Wybór ustawień w ramach Wyświetl nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.43 Filtr połączeń + SMS

Opcja **Filtr połączeń + SMS** zapewnia możliwość blokowania połączeń przychodzących oraz odbioru wiadomości tekstowych (SMS). Filtrowanie bazuje na zdefiniowanej przez użytkownika liście numerów telefonów.

Ocena ryzyka

Wybór ustawień w ramach **Filtr połączeń + SMS** nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.



Rys. 54 Opcje ustawień **Filtr połączeń + SMS**

4.1.44 Ekran podglądu

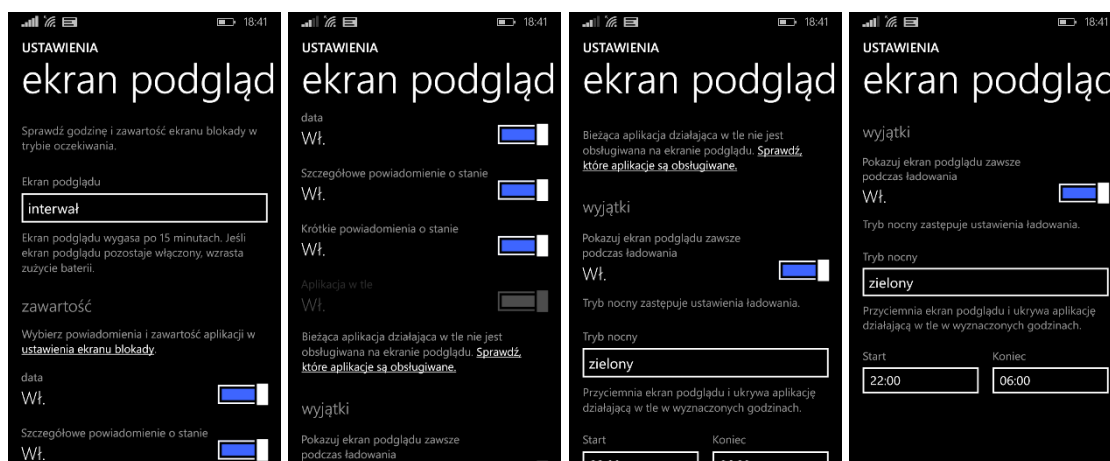
Opcja **Ekran podglądu** umożliwia wyświetlanie informacji pochodzących z aplikacji zainstalowanych na urządzeniu. Informacje wyświetlają się na ekranie urządzenia w czasie kiedy ekran przechodzi ze stanu aktywnego do stanu uśpienia.

Ocena ryzyka

- Wybór ustawień w ramach Ekranu podglądu mogą mieć wpływ na ujawnienie poufnych informacji przechowywanych w ramach aplikacji zainstalowanych na urządzeniu. .

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Ekran podglądu	Wył. Podejrzaj Interwał Zawsze Włączone	Interwał	Wył.

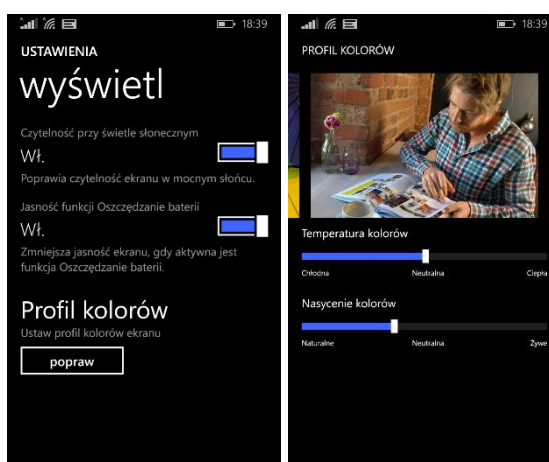


Rys. 55 Opcje ustawień *Ekran podglądu*

4.1.45 Wyświetl

W ramach ustawień dostępne są opcje umożliwiające konfigurację:

- konfiguracji czytelności przy świetle słonecznym,
- ustawienia jasności funkcji Oszczędzanie baterii,
- ustawienia profili kolorów ekranu.



Rys. 56 Opcje ustawień opcji *Wyświetl*

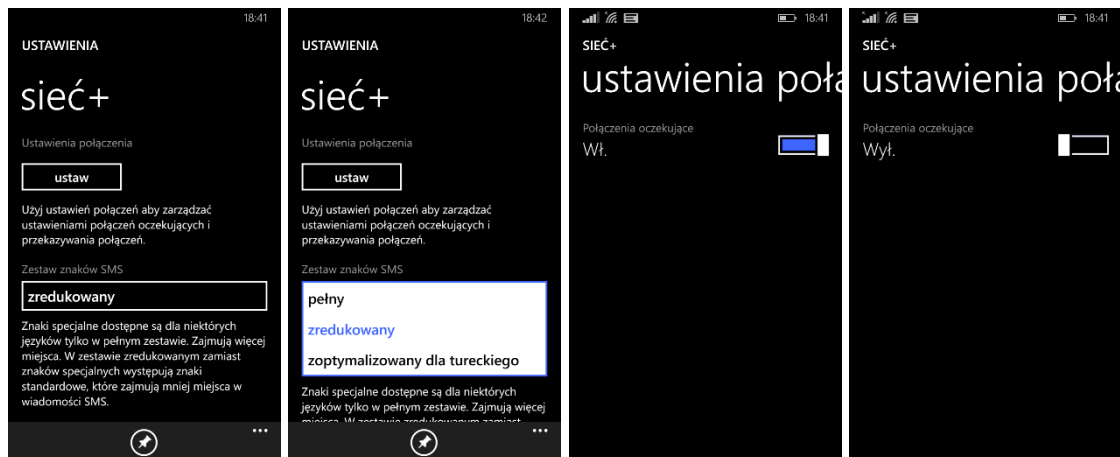
Ocena ryzyka

Wybór ustawień w ramach **Wyświetl** nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.46 Sieć +

Ustawienia **Sieć +** umożliwiają wykonanie:

- konfiguracji ustawień połączeń oczekujących i przekazywania połączeń,
- możliwość ustawienia zestawu znaków SMS,
- uzyskanie informacji o operatorze i ustawieniach karty SIM.



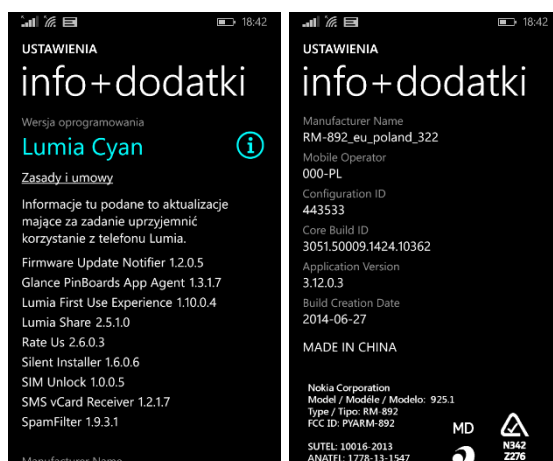
Rys. 57 Opcje ustawień **sieć +**

Ocena ryzyka

Wybór ustawień w ramach **Sieć +** nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.1.47 Info + dodatki

W ramach sekcji dostępne są szczegółowe informacje na temat oprogramowania, urządzenia oraz zasady i obowiązujące umowy.



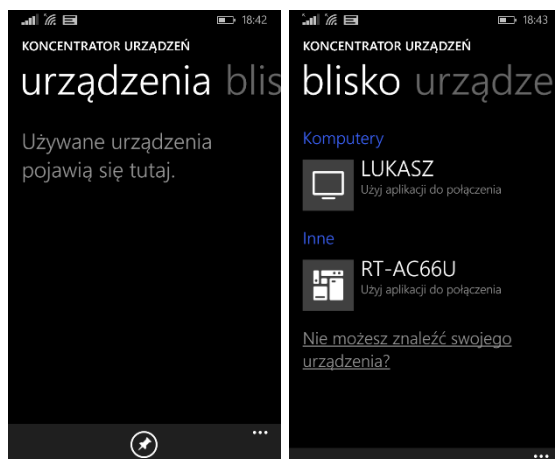
Rys. 58 Opcja **info + dodatki**

Ocena ryzyka

Sekcja **Info + dodatki** stanowi źródło informacji bez możliwości konfiguracji więc nie ma wpływu na opcje zabezpieczeń.

4.1.48 Koncentrator urządzeń

Koncentrator urządzeń umożliwia podłączanie innych telefonów, akcesoriów, tabletów, komputerów, konsol do gier, telewizorów, drukarek i innych urządzeń oraz zarządzania nimi.



Rys. 59 Opcje ustawień **Koncentrator urządzeń**

Ocena ryzyka

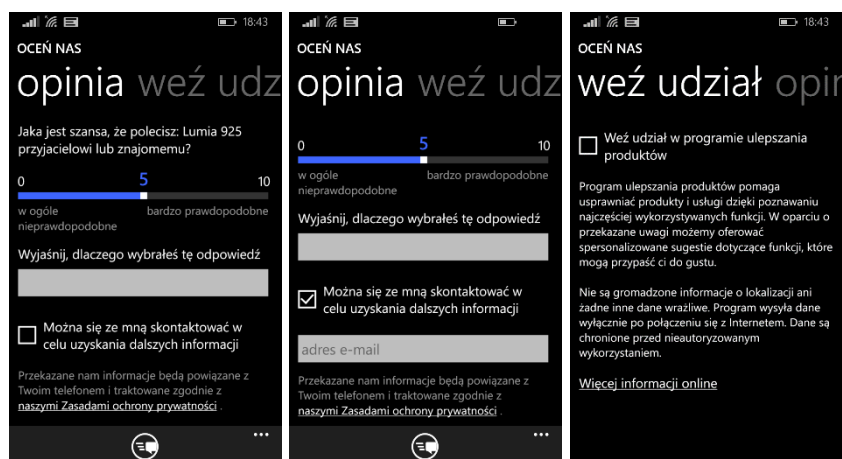
- Włączenie funkcji powoduje, że dane osobiste są wysyłane z urządzenia do źródeł korzystających z omawianych opcji.
- Korzystanie z opcji może wiązać się z synchronizacją wybranych ustawień do innych urządzeń. W przypadku nieuprawnionego do nich dostępu stanowi to potencjalne źródło wycieku informacji poufnych oraz osobistych użytkownika.
- Włączenie opcji powoduje domyślnie włączenie lokalizacji telefonu. Włączenie funkcji lokalizacji zwiększa transfer danych oraz powoduje, że dane osobiste są wysyłane z urządzenia do źródeł korzystających z omawianych opcji.

Minimalizacja ryzyka

Przed włączeniem opcji **Koncentrator urządzeń** należy zweryfikować zakres ustawień i rodzaj danych, które będą synchronizowane z podłączonymi urządzeniami.

4.1.49 Oceń nas

Ustawienia umożliwiają wyrażenie opinii dotyczącej używanego telefonu oraz konfigurację udziału w programie ulepszania produktów.



Rys. 60 Ustawienia opcji *Oceń nas*

Ocena ryzyka

- Ustawienie udziału w programie ulepszania produktów wiąże się z przekazywaniem firmom Nokia i Microsoft informacji dotyczących sposobu wykorzystywania urządzenia, aplikacji i usług dostępnych w telefonie. Należą do nich takie dane jak model urządzenia, nazwa operatora, kraj, unikatowy identyfikator urządzenia, poziom naładowania baterii, działanie podłączonych akcesoriów, informacje o błędach, opinie i oceny użytkowników. W ramach programu nie są gromadzone dane i zawartość wiadomości e-mail, SMS, dokumenty, notatki, wyszukiwania, zawartość plików multimedialnych czy dane o lokalizacji.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Weź udział w programie ulepszania produktów	Wł. Wył.	Wł.	Wył.

4.2 Ustawienia aplikacji

Ustawienia aplikacji mają istotny związek z aspektami bezpieczeństwa urządzeń Windows Phone. Ich konfiguracja odbywa się z poziomu **Ustawienia > Aplikacje** i obejmuje Internet Explorer, kontakty, mapy, Office, portfel, sklep, telefon, wiadomości, wyszukiwanie oraz zdjęcia + aparat.



Rys. 61 Ustawienia z podziałem na aplikacje

4.2.1 Internet Explorer

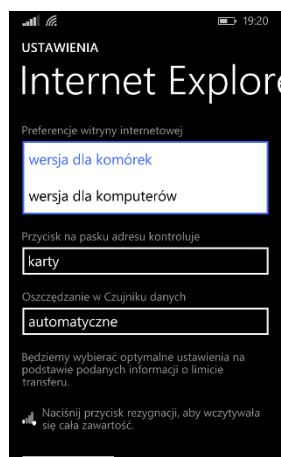
Sekcja umożliwia konfigurację przeglądarki Internet Explorer.



Rys. 62 Ustawienia Internet Explorer

4.2.1.1 Preferencje witryny internetowej

W zależności od ustawienia wyświetlanie witryn odbywa się w trybie dla telefonów lub dla komputerów.



Rys. 63 Ustawienia *Internet Explorer* - wybór wersji

Ocena ryzyka

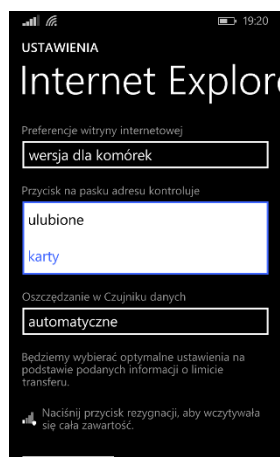
- Wybór ustawienia może wpływać na opcje zabezpieczeń urządzenia z uwagi na różnice w wykorzystywanych technologiach WWW.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Preferencje witryny internetowej <u>Uwaga:</u> Stosowanie opcji dla komórek uniemożliwia dostęp do witryn WWW przeznaczonych dla komputerów co może ograniczać dostęp do pożądaných treści.	Wersja dla komórek Wersja dla komputerów	Wersja dla komórek	Wersja dla komórek

4.2.1.2 Przycisk na pasku adresu kontroluje

Ustawienia umożliwia określenie zachowania się przycisku po lewej stronie od paska adresu. Do wyboru jest opcja Ulubione lub Karty.



Rys. 64 Ustawienia *Internet Explorer* - przycisk na pasku adresu

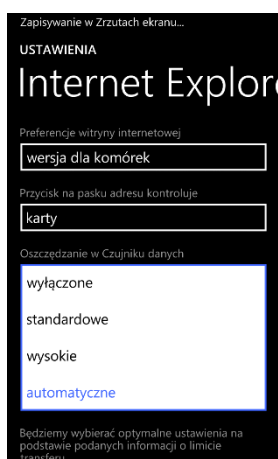
Ocena ryzyka

Wybór ustawienia nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.

4.2.1.3 Oszczędzanie w Czujniku danych

Ustawienie odpowiada za ilość wyświetlanych treści w trakcie przeglądania witryn WWW w ramach poniższych opcji:

- Wyłączone (Będziemy pobierać pełne strony),
- Standardowe (Będziemy lekko kompresować obrazy na stronach),
- Wysokie (Będziemy mocno kompresować obrazy, blokować niektóre reklamy i pobierać tylko fragmenty stron),
- Automatyczne (Będziemy wybierać optymalne ustawienia na podstawie podanych informacji o limicie transferu).



Rys. 65 Ustawienia *Internet Explorer* - czujnik danych

Ocena ryzyka

- Ustawienie ma wpływ na bezpieczeństwo z uwagi na możliwość określenia ilości wyświetlanych (a tym samym pobieranych) treści z witryn WWW, w tym reklam i obrazów.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Oszczędzanie w Czujniku danych <u>Uwaga:</u> Stosowanie opcji Wysokie ma wpływa na ilość prezentowanych danych w trakcie przeglądania witryn WWW i może spowodować brak dostępu do koniecznych informacji.	Wyłączone (Będziemy pobierać pełne strony) Standardowe (Będziemy lekko kompresować obrazy na stronach) Wysokie (Będziemy mocno kompresować obrazy, blokować niektóre reklamy i pobierać tylko fragmenty stron) Automatyczne (Będziemy wybierać optymalne ustawienia na podstawie podanych informacji o limicie transferu)	Wyłączone	Wysokie

4.2.1.4 Usunąć historię

Opcja pozwala na wykasowanie historii przeglądania, plików cookie oraz tymczasowych plików internetowych. Dodatkowo można usunąć zapisane hasła.



Rys. 66 Ustawienia *Internet Explorer* - usuwanie historii

Ocena ryzyka

- Ustawienie ma wpływ na bezpieczeństwo z uwagi na fakt, że w przechowywanych w pamięci podręcznej danych mogą znajdować się informacje poufne oraz prywatne.

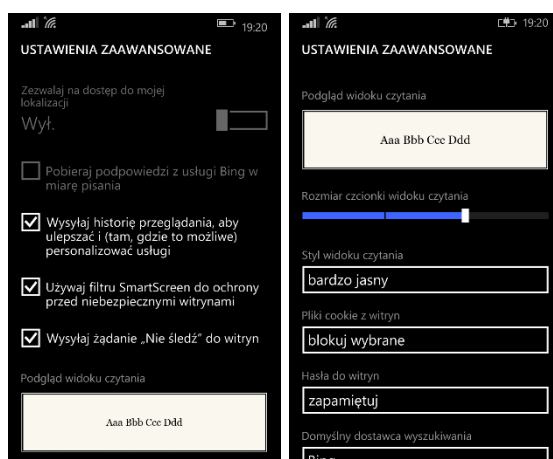
Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
-------	-------------------------	---------------------	--------------------------

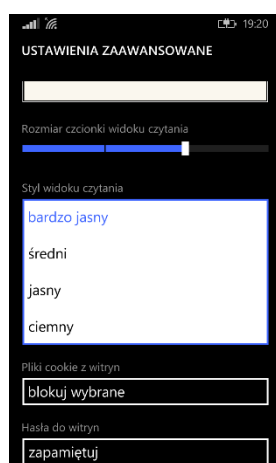
Usuń historię <u>Uwaga:</u> Trzymając historię przeglądania użytkownik ma szybszy dostęp do witryn oraz przy zastosowaniu opcji pamiętania haseł jest zwolniony z konieczności każdorazowego uwierzytelnienia.	-	-	Zaleca się cykliczne usuwanie historii przeglądania (min. co 30 dni)
---	---	---	--

4.2.1.5 Ustawienia zaawansowane

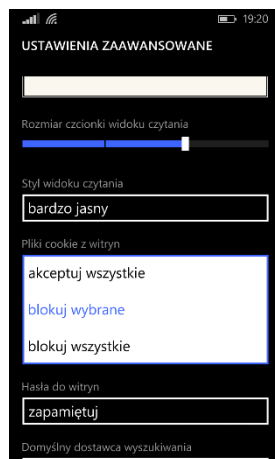
Ustawienia zaawansowane pozwalają na włączenie lokalizacji, wyrażenie zgody na wysyłanie historii przeglądania, wykorzystywanie filtru SmartScreen do ochrony przed niebezpiecznymi witrynami, konfigurację opcji Wysyłaj żądania „Nie śledź” do witryn, ustawienia opcji czytania, ustawienia plików cookie, konfigurację pamiętania haseł, wybór domyślnego dostawcę wyszukiwania oraz zezwolenie witrynom na przechowywanie plików w telefonie.



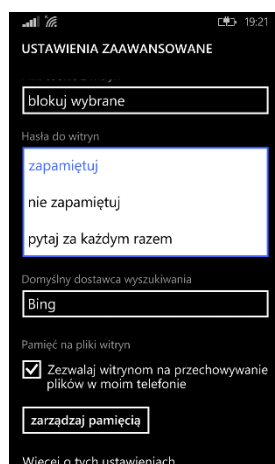
Rys. 67 Ustawienia zaawansowane Internet Explorer



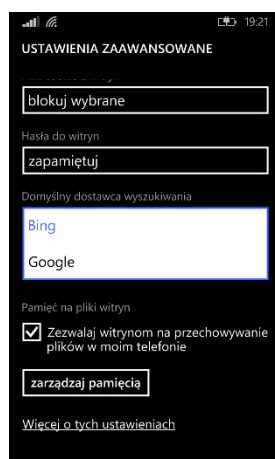
Rys. 68 Ustawienia zaawansowane Internet Explorer - styl widoku czytania



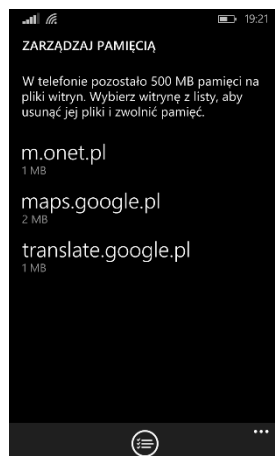
Rys. 69 Ustawienia zaawansowane Internet Explorer - pliki cookie z witryn



Rys. 70 Ustawienia zaawansowane Internet Explorer - hasła do witryn



Rys. 71 Ustawienia zaawansowane Internet Explorer - domyślny dostawca wyszukiwania



Rys. 72 Ustawienia zaawansowane Internet Explorer - zarządzanie pamięcią w urządzeniu

Ocena ryzyka

- Włączenie opcji wysyłania historii ma na celu pomoc w ulepszaniu usług Bing firmy Microsoft.
- Wykorzystywanie filtra SmartScreen zapewnia uzyskiwanie ostrzeżeń o witrynach, które zostały zgłoszone jako niebezpieczne lub podejrzane.
- Korzystanie z opcji Wysyłaj żądanie „Nie śledź” do witryn powoduje informowanie witryn internetowych, że nie chcesz aby przeglądanie stron było śledzone.
- Styl widoku czytania umożliwia dopasowanie opcji wyświetlania dłuższych tekstów i może mieć wpływ na wyciek danych w przypadku ryzyka podejrzenia przez osoby postronne wyświetlanych informacji.
- Konfiguracja plików cookie ma wpływ na poziom ich akceptacji przez Internet Explorer. Pliki cookie zapisują informacje, które mogą umożliwiać kontakt z użytkownikiem bez wyraźnej zgody.
- Ustawienia domyślnego dostawcy wyszukiwania nie ma wpływu na opcje zabezpieczeń gdyż są one niezależne od dokonanej w tym zakresie konfiguracji.
- Konfiguracja opcji zezwalającej na przechowywanie przez witryny plików w telefonie wiąże się z trzymaniem takich danych, jak niedokończone wiadomości e-mail czy źródła RSS w pamięci telefonu.

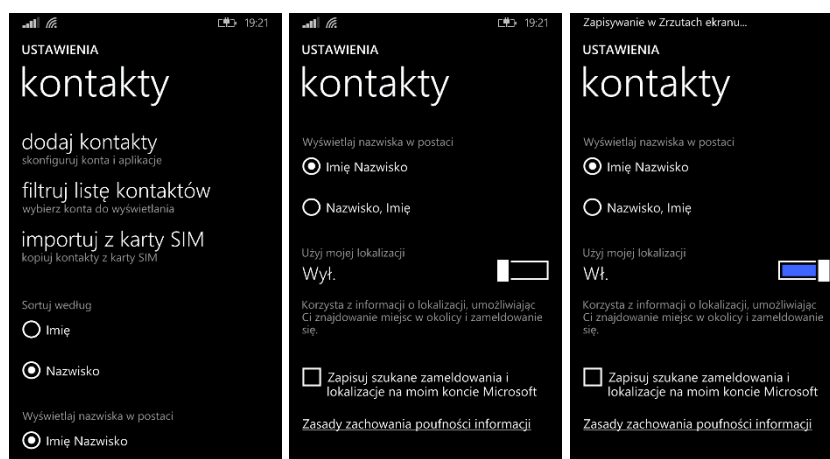
Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Zezwalaj na dostęp do mojej lokalizacji	Wł. Wył.	Wł.	Wył.
Wysyłaj historię przeglądania, aby ulepszać i (tam, gdzie to możliwe) personalizować usługi	Wł. Wył.	Wył.	Wył.
Używaj filtra SmartScreen do ochrony przed niebezpiecznymi witrynami	Wł. Wył.	Wył.	Wł.
Wysyłaj żądanie „Nie śledź” do witryn <u>Uwaga:</u> Mimo wybrania tego ustawienia niektóre witryny mogą nadal działać w	Wł. Wył.	Wł.	Wł.

sposób, który uznaje się za śledzenie. Zależy to praktyk stosowanych przez poszczególne witryny.			
Pliki cookie z witryn	Akceptuj wszystkie Blokuj wybrane Blokuj wszystkie	Blokuj wybrane	Blokuj wszystkie
Hasła do witryn	Zapamiętuj Nie zapamiętuj Pytaj za każdym razem	Pytaj za każdym razem	Nie zapamiętuj
Zezwalaj witrynom na przechowywanie plików w moim telefonie	Wł. Wył.	Wył.	Wył.
Stosowanie filtrów prywatyzujących zapobiegających odczytywanie wyświetlanych informacji przez osoby postronne.	-	-	-

4.2.2 Kontakty

Opcje umożliwiają dostosowanie ustawień w zakresie filtrowania listy kontaktów, ich sortowania oraz kolejności wyświetlania nazwisk. Dostępna jest również opcja włączenia używania lokalizacji co pozwala na odnajdywanie miejsc w okolicy i meldowania się. Dodatkowo istnieje możliwość zapisywania wyszukanych zameldowań o lokalizacji w ramach konta Microsoft.



Rys. 73 Ustawienia opcji **Kontakty**

Ocena ryzyka

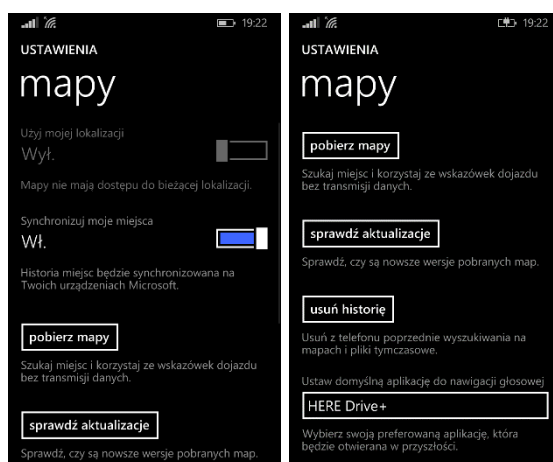
- Włączenie lokalizacji w opcji **Kontakty** powoduje, że użytkownik może korzystać z informacji o lokalizacji co przekłada się na dostęp do opcji odnajdywania miejsc w okolicy i meldowania się.
- Włączenie funkcji lokalizacji zwiększa transfer danych oraz powoduje, że dane osobiste są wysyłane z urządzenia do źródeł korzystających z omawianych opcji.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Użyj mojej lokalizacji	Wł. Wył.	Wł.	Wył.
Zapisuje znalezione zameldowania i lokalizacje na moim koncie Microsoft	Wł. Wył.	Wł.	Wył.

4.2.3 Mapy

Opcje umożliwiają udostępnienie lokalizacji urządzenia dla map oraz synchronizację miejsc użytkownika. Dodatkowo istnieje możliwość pobierania map, sprawdzania aktualizacji, usuwania historii wyszukiwania na mapach oraz plików tymczasowych jak i ustawienie domyślnej aplikacji dla nawigacji głosowej.



Rys. 74 Ustawienia aplikacji *Mapy*



Rys. 75 Ustawienia aktualizacji aplikacji *Mapy*

Ocena ryzyka

- Włączenie lokalizacji w opcji **Mapy** powoduje, że użytkownik może korzystać z lokalizacji w przypadku wykorzystywania map.
- Włączenie synchronizacji miejsc użytkownika powoduje, że historia będzie synchronizowana na urządzeniach Microsoft.

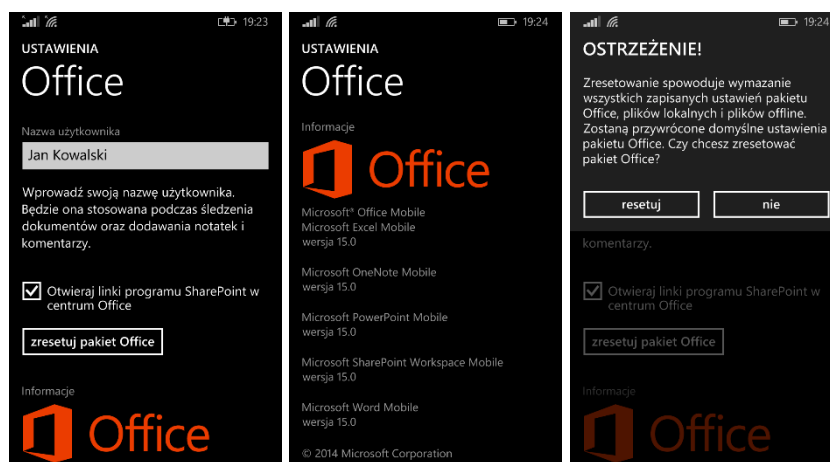
- Włączenie funkcji zwiększa transfer danych oraz powoduje, że dane osobiste są wysyłane z urządzenia do źródeł korzystających z omawianych opcji.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Użyj mojej lokalizacji <u>Uwaga:</u> W przypadku zapewnienia dostępu dla użytkownika lub aplikacji do map należy rozważyć zasadność włączenia opcji lokalizacji.	Wł. Wył.	Wł.	Wył.
Synchronizuj moje miejsca	Wł. Wył.	Wł.	Wł.
Usuń historię	-	-	Zaleca się cykliczne usuwanie historii i plików tymczasowych

4.2.4 Office

W ramach ustawień istnieje możliwość skonfigurowania nazwy użytkownika, zaznaczenia opcji umożliwiającej otwieranie linków programu SharePoint w centrum Office oraz zresetowanie pakietu Office.



Rys. 76 Ustawienia aplikacji Office

Ocena ryzyka

- Ustawienie nazwy użytkownika powoduje, że będzie ona wykorzystywana podczas śledzenia dokumentów oraz dodawania notatek i komentarzy.
- Włączenie opcji Otwieraj linki programu SharePoint w centrum Office umożliwia bezpośrednie kierowanie do lokalizacji witryn WWW. Tym samym istnieje ryzyko, że użytkownik może zostać przekierowany do strony zawierającej niechciane treści.

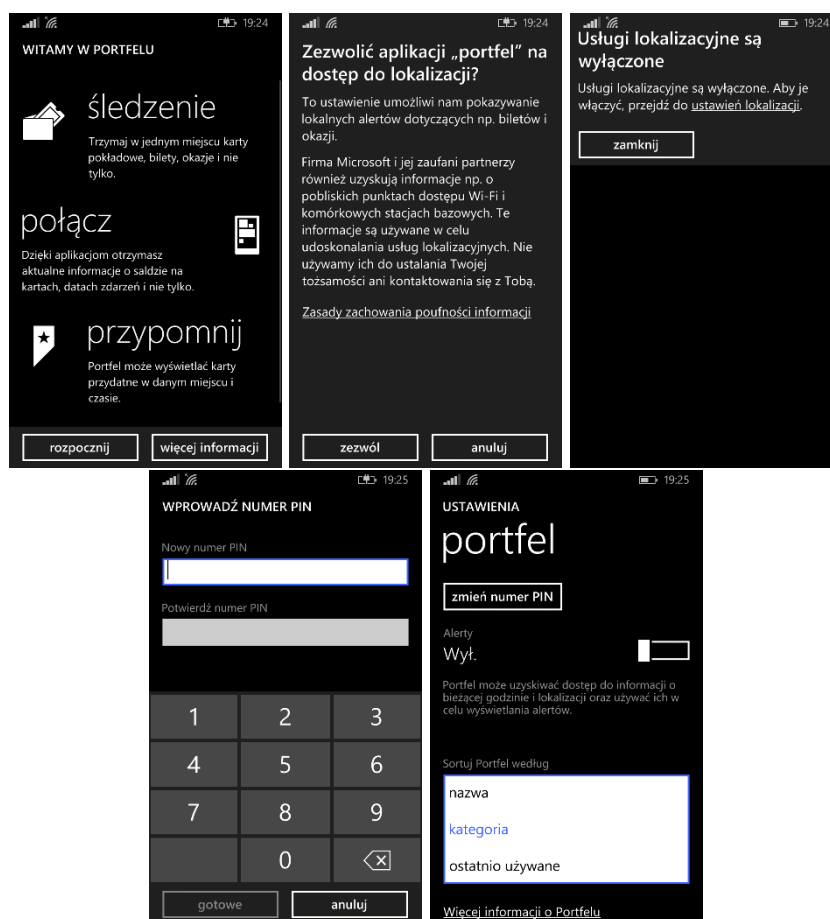
Proces minimalizacji ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
-------	-------------------------	---------------------	--------------------------

Otwieraj linki programu SharePoint w centrum Office <u>Uwaga:</u> W przypadku zapewnienia dostępu dla użytkownika lub aplikacji do lokalizacji SharePoint należy rozważyć zasadność włączenia opcji lokalizacji.	Wł. Wył.	Wł.	Wył.
Nazwa użytkownika	-	Użytkownik	Imię i nazwisko użytkownika urządzenia

4.2.5 Portfel

Portfel to miejsce do przechowywania cyfrowych wersji kart, kuponów, biletów, bonów upominkowych Sklepu Windows i Xbox itp. Dodawanie obiektów do portfela może odbywać się poprzez konto Microsoft, załącznik wiadomości email oraz przystosowanych do tego aplikacji.



Rys. 77 Ustawienia aplikacji *Portfel*

Ocena ryzyka

- Korzystanie z opcji **Portfel** z uwagi na śledzenie informacji o saldach może stanowić źródło informacji o stanie kont użytkownika.
- W powiązaniu z opcjami płatności za pomocą telefonu może narazić na utratę gotówki.

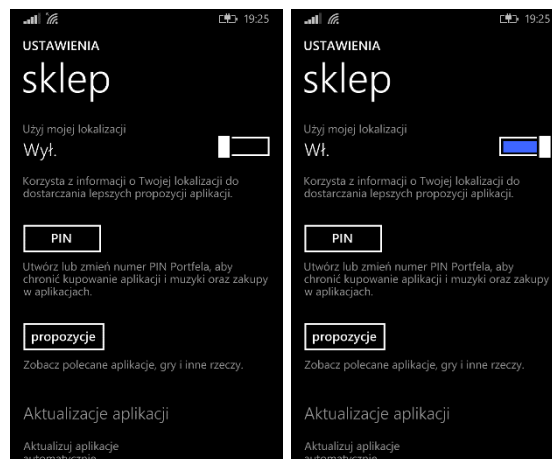
- Dodatkowo włączenie opcji lokalizacji zwiększa transfer danych oraz powoduje, że dane osobiste są wysyłane z urządzenia do źródeł korzystających z omawianych opcji.

Minimalizacja ryzyka

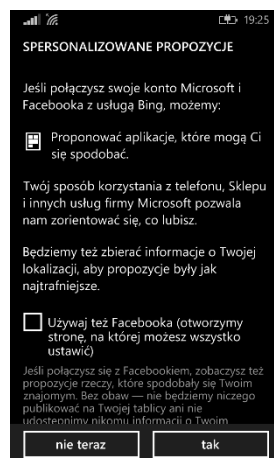
Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Numer PIN portfela <u>Uwaga:</u> w przypadku korzystania z opcji Portfel zaleca się stosowanie kodu PIN o długości minimum 8 cyfr oraz zachowanie cyklicznej zmiany kodu PIN minimum co 30 dni.	Wł. Wył.	Wł.	Wył.
Alerty	Wł. Wył.	Wł.	Wył.

4.2.6 Sklep

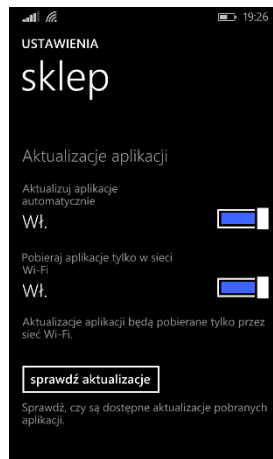
Sklep stanowi centrum firmy Microsoft umożliwiające użytkownikom przeglądanie i pobieranie aplikacji oraz gier na urządzenia z systemem Windows Phone.



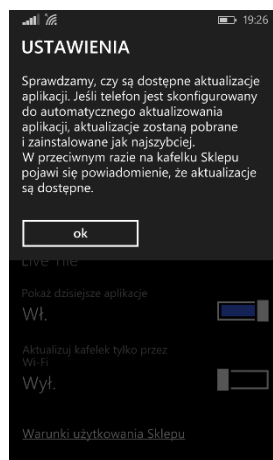
Rys. 78 Włączenie i wyłączenie używania lokalizacji w aplikacji **Sklep**



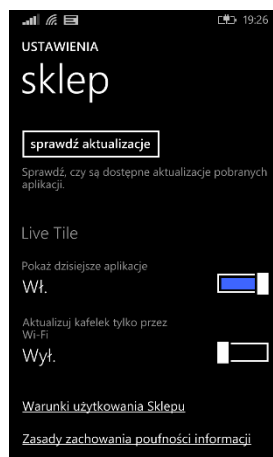
Rys. 79 Ustawienia spersonalizowanych propozycji w ramach aplikacji **Sklep**



Rys. 80 Włączenie automatycznych aktualizacji aplikacji



Rys. 81 Uruchomienie automatycznych aktualizacji aplikacji



Rys. 82 Ustawienia aplikacji Sklep

Ocena ryzyka

- Wykorzystywanie funkcji **Sklep** wiąże się z możliwością instalacji oprogramowania, pobierania muzyki oraz dokonywania zakupów w ramach posiadanych aplikacji.

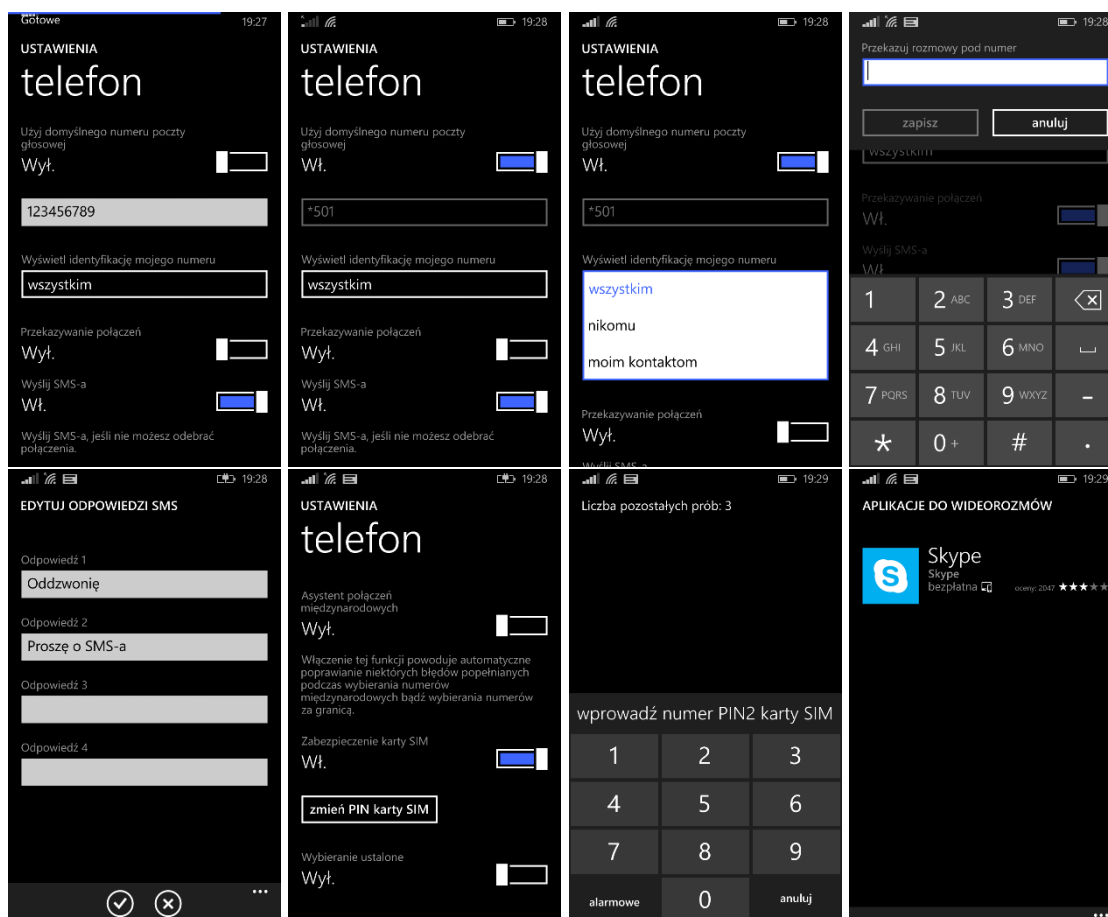
- Wśród dostępnych opcji znajdują się ustawienia aktualizacji aplikacji oraz dopasowania propozycji dla korzystającego z nich użytkownika co przekłada się na zwiększenie transferu danych.
- Włączenie opcji lokalizacji zwiększa transfer danych oraz powoduje, że dane osobiste są wysyłane z urządzenia do źródeł korzystających z omawianych opcji.
- W powiązaniu z kontem Microsoft oraz opcją **Portfel** istnieje ryzyko łatwego zakupu oprogramowania przez osoby, które uzyskały dostęp do urządzenia co może narazić na utratę gotówki.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Użyj mojej lokalizacji	Wł. Wył.	Wył.	Wył.
PIN	-	-	Zgodnie z wytycznymi w punkcie 4.2.5 Portfel
Aktualizuj aplikacje automatycznie	Wł. Wył.	Wł.	Wł.
Pobieraj aplikacje tylko w sieci Wi-Fi	Wł. Wył.	Wł.	Wł.

4.2.7 Telefon

W ramach opcji **Telefon** można dokonać modyfikacji ustawień dotyczących domyślnego numeru poczty głosowej, przekazywania połączeń, asystenta ustawień międzynarodowych oraz zabezpieczania karty SIM.



Rys. 83 Ustawienia opcji Telefon

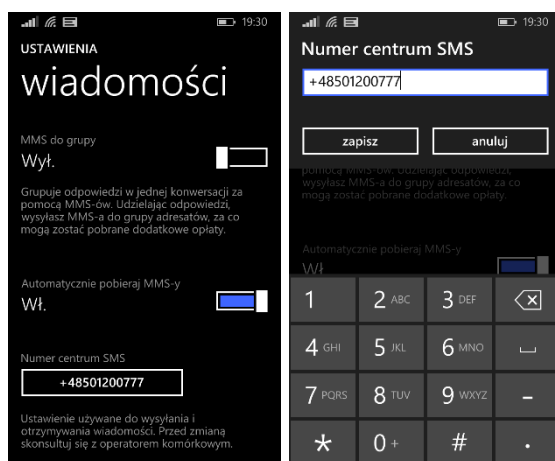
Ocena ryzyka

- Korzystanie z poczty głosowej wiąże się z nawiązywaniem połączenia w celu odsłuchania nagranych wiadomości. W przypadku zmiany numeru poczty głosowej może wiązać się z poniesieniem dodatkowych kosztów lub przekierowaniem na numer nie będący właściwym źródłem zapisanych dla użytkownika urządzeń wiadomości.
- Stosowanie opcji przekazywania połączeń może narazić na ponoszenie dodatkowych opłat wynikających z rodzaju i przeznaczenia numeru, na które odbywa się przekierowanie.
- Zabezpieczenie karty SIM powoduje, że po każdym uruchomieniu telefonu będzie wyświetlany monit o wprowadzenie numeru PIN karty SIM. Dzięki takiemu ustawieniu można zapobiec nawiązywaniu nieupoważnionych połączeń telefonicznych przez inne osoby.
- Wykorzystywanie asystenta połączeń międzynarodowych powoduje automatyczne poprawianie niektórych błędów popełnianych podczas wybierania numerów międzynarodowych bądź wybierania numerów za granicą. Włączenie opcji może uchronić przed narażeniem na poniesienie dodatkowych kosztów w przypadku błędów związanych z wybieraniem numerów w lokalizacji zagranicznej.
- Stosując wybieranie ustalone można ograniczyć możliwość nawiązywania połączeń, zezwalając tylko na połączenia z określonymi numerami telefonów. Do włączania/wyłączania wybierania ustalonego i do edycji kontaktów takiego wybierania potrzebny jest kod PIN2.

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Użyj domyślnego numeru poczty głosowej	Numer domyślny Numer wprowadzony przez użytkownika	Zależą od operatora GSM	Numer domyślny
Przekazywanie połączeń	Wył. Przekazuj rozmowy pod numer	Wył.	Wył.
Asystent połączeń międzynarodowych	Wył. Wł.	Wył.	Wł.
Zabezpieczenie karty SIM	Wył. Wł.	Wł.	Wł.
Wybieranie ustalone	Wył. Włącz wybier. ustalone - Włącza funkcję wybierania ustalonego. Wyłącz ustal. wybieranie - Wyłącza funkcję wybierania ustalonego. Nowy kontakt SIM - Wprowadź opis i numer telefonu kontaktu, do którego połączenia są dozwolone. Dodaj z Kontaktów - Umożliwia skopiowanie na listę wybierania ustalonego kontaktu z listy kontaktów.	Wył.	Wył.

4.2.8 Wiadomości

W ramach sekcji dostępne są ustawienia umożliwiające korzystanie z kopii zapasowej SMS-ów, potwierdzeń dostarczania SMS/MMS, wysyłania potwierdzeń otrzymania wiadomości MMS, grupowania odpowiedzi konwersacji za pomocą MMS-ów oraz ustawienie numeru centrum SMS.



Rys. 84 Ustawienia *Wiadomości*

Ocena ryzyka

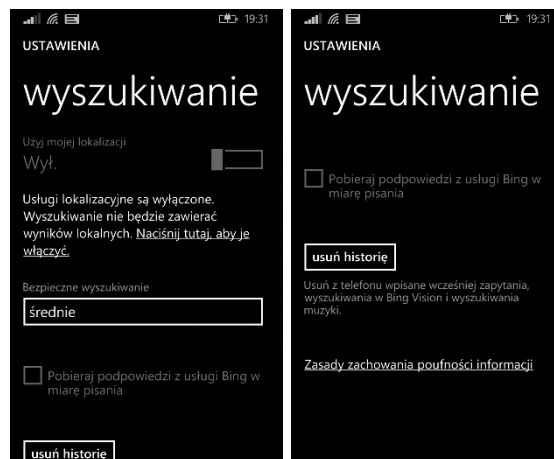
- Utrata danych należy do sytuacji krytycznych i dlatego zaleca się tworzenie kopii zapasowych. Dzięki tworzeniu kopii zapasowych SMS-ów i MMS-ów w chmurze można w łatwy sposób przywrócić konwersację przy konfiguracji nowego urządzenia. Wiadomości usuwane z telefonu są również kasowane z chmury, więc wszystkie dane są zawsze zsynchronizowane.
- Korzystanie z opcji potwierdzenia dostarczenia lub otrzymania wiadomości SMS/MMS ma na celu zagwarantowanie dostarczenia informacji. W zależności od operatora może wiązać się z dodatkowymi kosztami.
- Włączenie opcji automatycznego pobierania wiadomości MMS wiąże się ze zwiększonym transferem danych co może narazić na dodatkowe koszty.
- Konfiguracja niestandardowa numeru centrum SMS może spowodować przesyłanie danych osobistych do niezaufanych nadawców.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Kopia zapasowa SMS-ów	Wł. Wył.	Wył.	Wł.
Potwierdzenie dostarczenia SMS	Wł. Wył.	Wył.	Wył.
Potwierdzenie dostarczenia MMS	Wł. Wył.	Wył.	Wył.
Wyślij potwierdzenie otrzymania wiadomości MMS	Wł. Wył.	Wł.	Wył.
MMS do grupy	Wł. Wył.	Wył.	Wył.
Automatycznie pobieraj MMS-y	Wł. Wył.	Wył.	Wył.
Numer centrum SMS	Numer domyślny Numer wprowadzony przez użytkownika	Zależą od operatora GSM	Numer domyślny

4.2.9 Wyszukiwanie

W ramach ustawień można określić czy będzie wykorzystywana lokalizacja do poprawiania lokalnych wyników wyszukiwania, poziom bezpiecznego wyszukiwania, konfigurację podpowiedzi z usługi Bing oraz istnieje możliwość usunięcia historii zapytań w Bing Vision oraz wyszukiwania muzyki.



Rys. 85 Ustawienia opcji Wyszukiwania

Ocena ryzyka

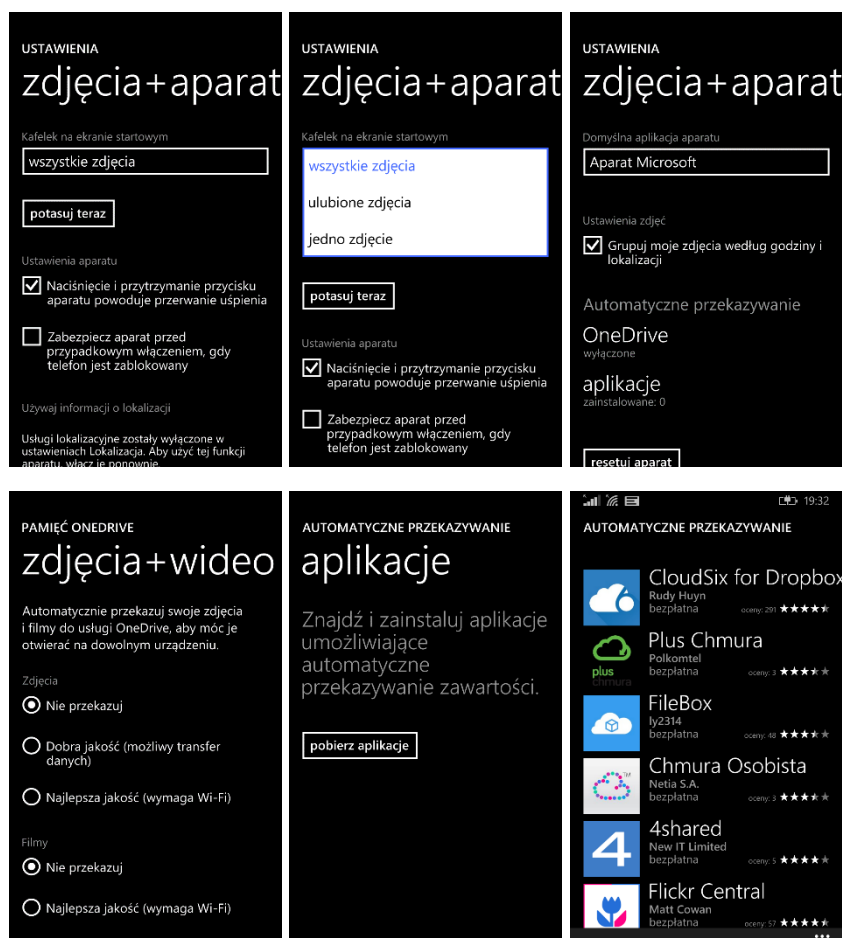
- Włączenie funkcji lokalizacji zwiększa transfer danych oraz powoduje, że dane osobiste są wysyłane z urządzenia do źródeł korzystających z omawianych opcji.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Użyj mojej lokalizacji	Wł. Wył.	Wył.	Wył.
Bezpieczne wyszukiwanie	Wyłączone Średnie Ścisłe		
Usuń historię <u>Uwaga:</u> Trzymając historię przeglądania użytkownik ma dostęp do wpisanych wcześniej wyszukiwanych terminów, danych usług Vision oraz wyszukiwania muzyki.	-	-	Zaleca się cykliczne usuwanie historii przeglądania (min. co 30 dni)

4.2.10 Zdjęcia + aparat

Opcje umożliwiają konfigurację kafelków zdjęć na ekranie startowym oraz ustawienia w zakresie reagowania przycisku aparatu, zabezpieczeń aparatu przed przypadkowym włączeniem, wykorzystywanie informacji o lokalizacji, konfigurację domyślnej aplikacji aparatu, możliwość grupowania zdjęć oraz automatycznego przekazywania do usługi OneDrive.



Rys. 86 Ustawienia opcji **Zdjęcia + aparat**

Ocena ryzyka

- Włączenie opcji przerywania uśpienia aparatu wiąże się z szybkim dostępem do aparatu a tym samym w przypadku braku zabezpieczenia telefonu kodem PIN również do wcześniej wykonanych zdjęć.
- Wyłączenie opcji zabezpieczenia aparatu przed przypadkowym włączeniem może spowodować nieprzewidziane scenariusze, które mogą prowadzić do nieplanowanego uruchomienia aplikacji lub nieświadomego wykorzystania funkcji urządzenia bez wiedzy użytkownika.
- Włączenie funkcji lokalizacji zwiększa transfer danych oraz powoduje, że do zdjęć i filmów będą dodawane informacje o lokalizacji.
- Włączenie opcji automatycznego przekazywania zdjęć i/lub filmów do biblioteki OneDrive użytkownika zwiększa transfer danych.

Minimalizacja ryzyka

Opcja	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Naciśnięcie i przytrzymanie przycisku aparatu	Wł. Wył.	Wł.	Wył.

powoduje przerwanie uśpienia			
Zabezpiecz aparat przed przypadkowym włączeniem, gdy telefon jest zablokowany	Wł. Wył.	Wył.	Wł.
Używaj informacji o lokalizacji	Wł. Wył.	Wł.	Wył.
Automatyczne przekazywanie OneDrive - Zdjęcia	Nie przekazuj Dobra jakość (możliwy transfer danych) Najlepsza jakość (wymaga Wi-Fi)	Nie przekazuj	Nie przekazuj
Automatyczne przekazywanie OneDrive - Filmy	Nie przekazuj Najlepsza jakość (wymaga Wi-Fi)	Nie przekazuj	Nie przekazuj

5. Konfiguracja urządzeń z Windows Phone w środowisku scentralizowanym

Zarządzanie zabezpieczeniami Windows Phone w modelu scentralizowanym jest możliwe z wykorzystaniem składowych pakietu Enterprise Mobility Suite. W skład rozwiązania wchodzi:

- Azure Active Directory Premium
Pozwala zarządzać użytkownikami ich tożsamością oraz dostępem do aplikacji i zasobów firmy znajdujących się zarówno w chmurze prywatnej jak i chmurze publicznej
- Windows Intune
Pozwala podłączyć do zasobów firmy dowolne urządzenie, odpowiednio je zabezpieczyć i kontrolować np. zdalnie usunąć dane w wypadku kradzieży.
- Azure Right Management Service
Pozwala zarządzać dostępem do informacji, zarówno wewnątrz firmy jak i poza nią, chronić dokumenty, wiadomości email czy biblioteki danych SharePoint poprzez ich szyfrowanie i restrykcyjne kontrolowanie uprawnień.

5.1 Konfiguracja ustawień zabezpieczeń w Windows Intune

Konfiguracja zabezpieczeń urządzeń z Windows Phone może być wykonana w modelu autonomicznym lub hybrydowym z wykorzystaniem System Center Configuration Manager.

Windows Intune oferuje zbiór zasad zabezpieczeń, które pozwalają na precyzyjne określenie ustawień dla urządzeń z Windows Phone w kategoriach:

- Hasła
- Szyfrowanie
- System
- Konta i synchronizacja
- Adres e-mail
- Przeglądarka
- Aplikacje
- Sprzęt
- Funkcje

5.1.1 Ustawienia zabezpieczeń haseł

Minimalizacja ryzyka

Zasada	Opis	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Wymagaj hasła do odblokowania urządzeń przenośnych	To ustawienie określa, czy użytkownicy mają wpisywać hasło przed uzyskaniem dostępu do informacji zapisanych na urządzeniu przenośnym	Wł. Wył.	Wł.	Wł.

	(niedostępne w systemie Windows RT)			
Wymagany typ hasła	To ustawianie określa czy hasła mogą składać się tylko z cyfr lub czy mogą zawierać inne znaki niż cyfry	Alfnumeryczne Numeryczne	Alfnumeryczne	Alfnumeryczne
Minimalna liczba zestawów znaków	Dostępne są cztery zestawy znaków: małe litery, duże litery, symbole i cyfry. Użyj tego parametru, aby określić minimalną liczbę zestawów znaków, które muszą się znajdować w hasle. Ustawienie wyższej wartości oznacza, że użytkownicy będą musieli używać bardziej skomplikowanych haseł.	1-4	1	3
Minimalna długość hasła	To ustawienie określa minimalną liczbę cyfr lub znaków hasła	1-14	4	7
Zezwalaj na proste hasła	To ustawienie określa czy na urządzeniach przenośnych można używać prostych haseł takich jak 1234 lub 1111.	Wł. Wył.	Wył.	Wył.
Liczba dopuszczalnych nieudanych logowań przed skasowaniem danych urządzenia	To ustawienie określa, ile razy można kolejno wpisać nieprawidłowe hasło, zanim wszystkie dane zostaną wyczyszczone z urządzenia przenośnego	4-11	4	4
Liczba minut braku	To ustawienie określa czas bezczynności,	1 min 5 min	15 min	1 min

aktywności przed wyłączeniem ekranu	po jakim następuje zablokowanie urządzenia przenośnego	15 min 30 min 1 godz.		
Wygaśnięcie hasła w dniach	To ustawienie określa czas, po jakim należy zmienić hasło urządzenia przenośnego	1-41 (w dniach)	41 dni	41 dni
Pamiętaj historię haseł	To ustawienie określa czy zezwalać na używanie poprzednich haseł.	Wł. Wył.	Wł.	Wł.
Zapobiegaj ponownemu używaniu poprzednich haseł	To ustawienie określa ile poprzednich haseł nie może być ponownie użytych przez użytkownika	1-24	5	5

5.1.2 Ustawienia szyfrowania

Minimalizacja ryzyka

Zasada	Opis	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Wymagaj szyfrowania na urządzeniu przenośnym	To ustawienie włącza szyfrowanie na urządzeniu przenośnym. Szyfrowanie nie można włączyć na niektórych urządzeniach.	Wł. Wył.	Wył.	Wł.
Wymagaj szyfrowania na kartach pamięci	To ustawienie określa, czy jest wymagane szyfrowanie danych na karcie pamięci urządzenia przenośnego.	Wł. Wył.	Wył.	Wył.

5.1.3 Ustawienia systemu

Minimalizacja ryzyka

Zasada	Opis	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Zezwalaj na przechwytywanie ekranu	Zezwalaj na przechwytywanie zawartości ekranu w postaci obrazu	Wł. Wył.	Wył.	Wył.
Zezwalaj na przesyłanie danych diagnostycznych	Zezwalaj urządzeniu przenośnemu na przesyłanie danych diagnostycznych.	Wł. Wył.	Wył.	Wył.

5.1.4 Ustawienia kont i synchronizacji

Minimalizacja ryzyka

Zasada	Opis	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Zezwalaj na korzystanie z konta Microsoft	Zezwalaj na połączenie konta Microsoft z urządzeniem przenośnym	Wł. Wył.	Wył.	Wł.

5.1.5 Ustawienia e-mail

Minimalizacja ryzyka

Zasada	Opis	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Zezwalaj użytkownikom na pobieranie załączników wiadomości e-mail (Exchange ActiveSync)	To ustawienie określa, czy na urządzenie przenośne można pobierać załączniki wiadomości e-mail	Wł. Wył.	Wył.	Wł.
Okres synchronizacji poczty e-mail (Exchange ActiveSync)	To ustawienie określa maksymalną liczbę dni, z których wiadomości e-mail mają być synchronizowane na urządzeniu przenośnym	Wył. 1 dzień 3 dni 1 tydzień 2 tygodnie 1 miesiąc Bez limitu	Wył.	3 dni
Zezwalaj urządzeniom przenośnym, które nie	To ustawienie określa, czy program Exchange może obsługiwać dostęp	Wł. Wył.	Wył.	Wł.

obsługują w pełni tych ustawień, na synchronizowanie z programem Exchange (Exchange ActiveSync)	do urządzeń przenośnych, które nie obsługują niektórych lub wszystkich wybranych ustawień programu Exchange ActiveSync			
Zezwalaj na niestandardowe konta e-mail	Zezwalaj urządzeniu przenośnemu na synchronizowanie danych z kontami e-mail innych firm	Wł. Wył.	Wył.	Wł.

5.1.6 Ustawienia przeglądarki

Minimalizacja ryzyka

Zasada	Opis	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Zezwalaj na działanie przeglądarki sieci Web	To ustawienie określa, czy jest dozwolone używanie przeglądarki sieci Web urządzenia przenośnego.	Wł. Wył.	Wył.	Wł.

5.1.7 Ustawienia aplikacji

Minimalizacja ryzyka

Zasada	Opis	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Zezwalaj na dostęp do sklepu z aplikacjami	Zezwalaj na korzystanie ze sklepu z aplikacjami na urządzeniu przenośnym	Nie skonfigurowane Wł. Wył.	Wył.	Wł.

5.1.8 Ustawienia sprzętu

Minimalizacja ryzyka

Zasada	Opis	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Zezwalaj na korzystanie z aparatu	To ustawienie określa czy jest dozwolone używanie aparatu	Nie skonfigurowane Tak	Nie skonfigurowane	Tak

	urządzenia przenośnego	Nie		
Zezwalaj na używanie magazynu wymiennego	Zezwalaj urządzeniu przenośnemu na używanie magazynu przenośnego	Nie skonfigurowane Tak Nie	Nie skonfigurowane	Tak
Zezwalaj na sieć Wi-Fi	Zezwalaj na używanie sieci Wi-Fi na urządzeniu przenośnym.	Nie skonfigurowane Zabronione Dozwolone	Nie skonfigurowane	Zabronione
Zezwalaj na udostępnianie połączenia internetowego przez Wi-Fi	Zezwalaj na udostępnianie połączenia Wi-Fi na urządzeniu przenośnym.	Nie skonfigurowane Wyłączone Włączono	Nie skonfigurowane	Wyłączone
Zezwalaj na automatyczne połączenia z bezpłatnymi punktami hotspot Wi-Fi	Zezwalaj urządzeniu przenośnemu na automatyczne łączenie się z publicznymi punktami hotspot Wi-Fi i akceptowanie wszystkich wymaganych warunków użytkownika	Nie skonfigurowane Wyłączone Włączono	Nie skonfigurowane	Wyłączone
Zezwalaj na raportowanie informacji o punktach hotspot Wi-Fi	Wysyłaj informacje dotyczące połączeń Wi-Fi w celu umożliwienia wykrycia sieci Wi-Fi w pobliżu.	Nie skonfigurowane Wyłączone Włączono	Nie skonfigurowane	Wyłączone
Zezwalaj na używanie funkcji geolokacji	Zezwalaj urządzeniu przenośnemu na wykorzystywanie informacji o lokalizacji	Nie skonfigurowane Nie Tak	Nie skonfigurowane	Nie
Zezwalaj na komunikacje NFC	Zezwalają na używanie komunikacji zbliżeniowej na urządzeniu przenośnym	Nie skonfigurowane Tak Nie	Nie skonfigurowane	Tak
Zezwalaj na połączenie Bluetooth	Zezwalaj na używanie interfejsu Bluetooth na urządzeniu	Nie skonfigurowane Tak Nie	Nie skonfigurowane	Tak

	przenośnym. Skonfigurowanie tego ustawienia na urządzeniu z systemem Windows Phone 8.1 nie spowoduje zmiany stanu urządzenia, ale umożliwi raportowanie zgodności dotyczącej tego ustawienia			
--	--	--	--	--

5.1.9 Ustawienia funkcji

Minimalizacja ryzyka

Zasada	Opis	Wartości konfiguracyjne	Ustawienie domyślne	Ustawienie rekomendowane
Zezwalaj na kopiowanie i wklejanie	Zezwalaj na kopiowanie i wklejanie na urządzeniu przenośnym.	Nie skonfigurowane Nie Tak	Nie skonfigurowane	Nie

6. Bezpieczeństwo danych

Windows Phone wykorzystuje w pełni opcje zabezpieczeń wynikające z możliwości sprzętowych urządzeń. Łącząc zabezpieczenia systemu operacyjnego z zabezpieczeniami na poziomie sprzętu osiąga się coraz większy poziom bezpieczeństwa danych.

Do zabezpieczeń na poziomie sprzętu które integrują się z systemem operacyjnym możemy zaliczyć:

- UEFI (Unified Extensible Firmware Interface) jest nowym standardem interfejsu oprogramowania układowego komputerów. Jest to następca dotychczasowego standardu BIOS (Basic Input/Output System). Implementacja UEFI występuje obecnie w prawie każdym nowym urządzeniu. Oprócz standardowej funkcjonalności jaką świadczy BIOS, UEFI posiada szereg nowych zaawansowanych funkcji. Główna zmiana nastąpiła w procesie startu systemu. Obecnie proces ten jest zabezpieczony przed modyfikacjami jakie mogą zostać wprowadzone przez złośliwe oprogramowanie. Zabezpieczenie polega na sprawdzeniu czy urządzenie posiada niezmodyfikowane, podpisane cyfrowo oprogramowanie układowe, które zostało wgrane przez producenta. Jedynie tylko producent urządzenia może wprowadzać autoryzowane zmiany w oprogramowaniu układowym.
- TPM (Trusted Platform Module) jest to procesor kryptograficzny wbudowany w wiele nowych urządzeń przenośnych takich jak laptopy czy telefony. Główną rolą tego procesora jest tworzenie i przechowywanie kluczy i skrótów kryptograficznych. Układ ten umożliwia podpisywanie danych za pomocą kluczy prywatnych. TPM może być wykorzystywany przez UEFI i system operacyjny jako bezpieczne miejsce do przechowywania informacji niezbędnych do weryfikacji czy integralności kluczy, skrótów kryptograficznych lub np. plików startowych. TPM jest również wykorzystywany do przechowywania kluczy i certyfikatów dla funkcji Bitlocker oraz wirtualnych kart inteligentnych np. stosowanych w uwierzytelnianiu wieloskładnikowym MFA (Multi-Factor Authentication). Obecnie wszystkie telefony z zainstalowanym w systemem Windows Phone 8.1 są wyposażone w moduł TPM.

6.1 Szyfrowanie

Zabezpieczenie poufnych i wrażliwych danych przechowywanych na urządzeniach mobilnych jest bardzo ważnym punktem w ramach polityki bezpieczeństwa przedsiębiorstwa, której postanowienia muszą obejmować wszystkie zagrożenia skutkujące utratą danych. System Windows Phone został wyposażony w zestaw technologii mających na celu ochronę danych, do których zaliczamy:

- szyfrowanie magazynu wewnętrznego,
- ochrona nośników zewnętrznych,
- zarządzanie prawami do informacji,
- szyfrowanie i podpisywanie S/MIME,
- szyfrowanie połączeń.

6.1.1 Szyfrowanie magazynu wewnętrznego

Windows Phone 8.1 zapewnia szyfrowanie danych przechowywanych na urządzeniu. Szyfrowanie oparte jest o technologie Bitlocker, która używa klucza Advanced Encryption Standard (AES) o długości 128-bitów. Klucz użyty do szyfrowania jest zabezpieczony za pomocą modułu TPM. Zapewnia to, że dane przechowywane na urządzeniu są zawsze bezpieczne, nawet w przypadku fizycznego dostępu do nich np. wymontowanie pamięci z urządzenia. Łącząc ze sobą szyfrowanie danych z zabezpieczeniami po stronie urządzenia, osiągamy bezpieczne miejsce przechowywania danych. Używając systemu MDM można wymusić żeby dane przechowywane na telefonach były zawsze szyfrowane (zasada Wymagaj szyfrowania danych). Kolejną zasadą zapobiegającą dostępowi do danych jest zasada wymuszająca wymazanie danych z urządzenia po kilkukrotnym błędnym wprowadzeniu kodu PIN (Liczba dopuszczalnych nieudanych logowań przed skasowaniem urządzenia).

6.1.2 Ochrona nośników zewnętrznych

Wiele telefonów również te wyposażone w system Windows Phone posiadają wbudowane gniazda kart pamięci. Od systemu Windows Phone 8.1 wspierane jest instalowanie aplikacji na kartach pamięci. Aplikacje są instalowane na specjalnie przygotowanej, zaszyfrowanej partycji na karcie pamięci. Funkcjonalność ta jest domyślnie włączona i nie wymaga dodatkowych ustawień. Rozwiązanie z podziałem karty pamięci na część zaszyfrowaną przeznaczoną dla aplikacji i na część nieszyfrowaną przeznaczoną na dane użytkownika, zwiększa to elastyczność użytkowania karty. Użytkownik może bez problemów przechowywać swoje dane na części przeznaczonej na dane prywatne. Jednocześnie dane aplikacji są bezpiecznie przechowywane na oddzielnej partycji.

Jeżeli obsługa kart wymiennych jest włączona, użytkownik może bezpośrednio wgrywać aplikacje jak i pobierać dane z karty. Używając tej funkcjonalności można instalować aplikacje, które są dostępne przez system MDM. Jednocześnie obowiązuje tu ta sama zasada co przy instalowaniu aplikacji np. z aplikacji Sklep. Aplikacje muszą być podpisane cyfrowo np. certyfikatem organizacji.

6.1.3 Zarządzanie prawami do informacji

Urządzenia z Windows Phone są jednymi z nielicznych telefonów, które wspierają obsługę zarządzania prawami informacji IRM (Information Rights Management). Umożliwia to obsługę na telefonie dokumentów zabezpieczonych za pomocą Windows RMS (Windows Rights Management Services). Dokumenty takie są zaszyfrowane i tylko uprawnione osoby mogą otworzyć je lub dokonywać dodatkowych operacji. Używając IRM można również ograniczać kopiowanie zawartości, drukowanie. W przypadku wiadomości e-mail zabezpieczonych RMS można nałożyć ograniczenia blokujące możliwość przesyłania dalej takich informacji. Usługa RMS skonfigurowana w ramach organizacji może być stosowana do ochrony informacji przechowywanych nie tylko jako treść lub załączniki wiadomości e-mail. Dokumenty przechowywane w ramach Microsoft SharePoint również mogą być objęte działaniem usługi RMS.

Zaimplementowana w system Windows Phone usługa zarządzania prawami informacji współdziała z usługami Microsoft Office 365 takimi jak

- SharePoint Online,
- Exchange Online.

Dział wsparcia w przedsiębiorstwie może włączyć obsługę IRM za pomocą systemu MDM lub Microsoft Exchange Server.

6.1.4 Szyfrowanie i podpisywanie S/MIME

Nowością w systemie Windows Phone 8.1 jest wsparcie dla S/MIME. Użytkownik może podpisywać i szyfrować wiadomości e-mail. Szyfrowana jest zawartość całej wiadomości a odszyfrowania może dokonać tylko uprawniona osoba lub grupy osób.

W celu konfiguracji podpisywania i szyfrowania za pomocą S/MIME należy włączyć poniższe zasady w systemie MDM lub w Microsoft Exchange Server:

- wymagaj podpisywania wiadomości S/MIME,
- wymagaj szyfrowania wiadomości S/MIME,
- wymagaj algorytmu podpisywania S/MIME,
- wymagaj algorytmu szyfrowania S/MIME,
- zezwalaj na negocjację algorytmu szyfrowania S/MIME,
- zezwalaj na S/MIME SoftCerts.

6.1.5 Szyfrowanie połączeń

Częstym sposobem na dostęp do informacji przez osoby nieupoważnione jest przechwycenie niezaszyfrowanych wiadomości przesyłanych między dwoma urządzeniami. W przypadku przesyłania w ten sposób informacji wymaganych do uwierzytelnienia np. w aplikacji bankowej osoba postronna otrzymuje pełne dane pozwalające na dostęp do informacji poufnych.

Windows Phone zawiera mechanizmy pozwalające na zabezpieczenie informacji wysyłanych do innych urządzeń. Jednymi z metod są:

- Szyfrowanie połączeń za pomocą protokołów TLS (Transport Layer Security) i SSL (Secure Sockets Layer). Większość serwisów WWW używa TLS i SSL do szyfrowania komunikacji. Windows Phone wspiera TLS w wersjach 1.0 do 1.2 oraz SSL w wersji 3.0. Urządzenie z Windows Phone dostarczane jest z zaufanymi certyfikatami, które mogą być używane do szyfrowania komunikacji. Ręcznie lub za pomocą systemów MDM mogą zostać wgrane do urządzenia nowe zaufane certyfikaty, np. certyfikat przedsiębiorstwa.
- Tworzenie bezpiecznych sieci VPN (Virtual Private Network). Ideą tworzenia sieci VPN jest połączenie w bezpieczny sposób dwóch sieci prywatnych używając jako nośnika sieci publicznej. Na przykład dostęp z sieci domowej do danych znajdujących się w sieci przedsiębiorstwa. W celu zapewnienia bezpieczeństwa połączenia VPN wymagane jest używanie szyfrowania transmisji. Urządzenia z Windows Phone 8.1 zapewniają ochronę połączeń VPN za pomocą protokołów IKEv2, IPsec oraz SSL. W przypadku gdy przedsiębiorstwo używa rozwiązań VPN-SSL dostarczonych przez firmy trzecie, w celu zapewnienia kompatybilności z Windows Phone należy pobrać dodatek producenta zapewniający wsparcie VPN-SSL dla Windows Phone.

6.2 Ochrona przed złośliwym oprogramowaniem

Urządzenia mobilne muszą być odporne na działanie złośliwego oprogramowania. W przypadku telefonów zagrożenie jest jeszcze większe ponieważ są to urządzenia często używane w publicznych

miejscach. Windows Phone wyposażony jest w szereg funkcji które pomagają chronić urządzenie przed nieautoryzowanym dostępem. W kolejnych punktach znajdują się szczegółowe opisy faz startu systemu.

6.2.1 Proces uruchamiania systemu

Windows Phone wykorzystuje niektóre mechanizmy wbudowane również w system Windows 8.1. Jednym z takich mechanizmów jest bezpieczny proces startu systemu (Secure Boot). Jest to właściwość UEFI, która chroni proces startu systemu przed ingerencją nieupoważnionych osób lub oprogramowania. Proces bezpiecznego startu przebiega w następujący sposób:

- urządzenie z Windows Phone uruchamia się
- oprogramowanie układowe urządzenia porównuje, czy cyfrowe sygnatury plików startowych Windows Phone są takie same jak podpisane i potwierdzone przez zaufany ośrodek certyfikacji sygnatury przechowywane w bazie UEFI,
- po spełnieniu powyższego warunku następuje załadowanie plików startowych systemu operacyjnego.

W urządzeniach z Windows Phone nie jest możliwe wyłączenie bezpiecznego startu systemu oraz wgrania innego systemu operacyjnego.

6.2.2 Zaufany proces uruchomienia systemu

Zabezpieczenia UEFI weryfikują pliki startowe systemu operacyjnego i uznają je za zaufane. Następnym etapem zabezpieczeń procesu uruchamiania systemu operacyjnego jest ochrona komponentów systemu. Weryfikacji podlega jądro systemu. W kolejnych krokach jądro systemu sprawdza czy są prawidłowe sygnatury poszczególnych składników takich jak sterowniki i pliki startowe. W przypadku napotkania zmodyfikowanych plików są one pomijane w procesie startu systemu.

6.2.3 Integralność systemu i aplikacji

Fazą następującą po prawidłowym załadowaniu plików systemowych jest automatyczny start aplikacji i komponentów systemu. Wszystkie aplikacje i komponenty systemu Windows Phone muszą być podpisane cyfrowo. Podpis może zostać wykonany przez twórcę aplikacji lub indywidualnie przez przedsiębiorstwo. Jeżeli aplikacje nie są podpisane lub zostały zmodyfikowane w nieautoryzowany sposób, system Windows Phone nie uruchamia ich. Wszystkie aplikacje dostępne w ramach aplikacji Sklep są podpisane cyfrowo. Wykorzystując tą cechę ogranicza się możliwość uruchamiania złośliwego oprogramowania.

Firma Microsoft dba o to żeby poziom zabezpieczeń w każdej nowej wersji systemu Windows był wyższy. Uwaga związana z bezpieczeństwem skupia się głównie na samym systemie operacyjnym. Jednakże na poziom bezpieczeństwa systemu mają bardzo duży wpływ zainstalowane na nim aplikacje. Windows Phone 8.1 został wyposażony w funkcje pozwalające ograniczyć ryzyko skompromitowania systemu przez działalność złośliwego oprogramowania. Wbudowane w Windows Phone 8.1 mechanizmy kontroli i izolacji aplikacji pozwalają ograniczyć zasięg szkód jakie może spowodować złośliwe oprogramowanie. Do mechanizmów i narzędzi podnoszących poziom bezpieczeństwa działania aplikacji w Windows Phone 8.1 należą:

- dostęp do oprogramowania przez aplikację Sklep,

- kontener aplikacji,
- ochrona aplikacji systemu operacyjnego,
- własne aplikacje biznesowe,
- portal firmy,
- Internet Explorer.

6.2.4 Sklep

Organizacje starają się o ograniczenie możliwości instalacji aplikacji z niezalecanych lub niebezpiecznych źródeł. Miejsca takie mogą zawierać aplikacje w które wbudowany jest kod złośliwego oprogramowania. Jednym z rozwiązań na uniknięcie instalacji aplikacji, która potencjalnie może zawierać złośliwe oprogramowanie jest używanie aplikacji Sklep. Wszystkie aplikacje zanim zostaną opublikowane w ramach Sklepu przechodzą wnikliwą analizę czy nie zawierają niepożądanego oprogramowania. Aplikacja po pomyślnym przejściu procesu weryfikacji zostaje podpisana cyfrowo. Dopiero zweryfikowana i podpisana jest dopuszczona do publikacji. Powyższy proces wpływa na ograniczenie możliwości przedostania się złośliwego oprogramowania.

Wiele aplikacji pochodzących ze Sklepu wymaga od użytkownika celem wyrażenia zgody na instalację oraz przesłanie poufnych informacji takich jak lokalizacja, nazwa użytkownika i hasło. Zasadą jest, że w takiej sytuacji następuje powiadomienie o tym użytkownika. Pomaga to podnieść świadomość użytkowników o wykorzystywaniu przez aplikację poufnych danych.

Ustawieniami Sklepu można zarządzać za pomocą scentralizowanych zasad w ramach przedsiębiorstwa (np. można całkowicie wyłączyć dostęp Sklepu).

6.2.5 Kontener aplikacji

Model zabezpieczeń Windows Phone jest oparty na zasadzie najmniejszych przywilejów i wykorzystuje izolację, aby go osiągnąć. Każda aplikacja pracująca w Windows Phone, również duże części systemu operacyjnego działają w ramach odizolowanych obszarów zwanych kontenerami aplikacji. W obszarach tych działają aplikacje i ich procesy. Każdy kontener jest zdefiniowany i utworzony za pomocą zasad zabezpieczeń. Zasady określają możliwości systemu operacyjnego do którego mają dostęp procesy w ramach kontenera. Możliwościami systemu są zasoby urządzenia z zainstalowanym Windows Phone – np. informacje o lokalizacji, kamera, mikrofon, czujniki, sieć.

Domyślnie minimalny poziom uprawnień jest dany każdemu kontenerowi aplikacji. Dostęp do dodatkowych możliwości systemu może zostać zdefiniowany w kodzie aplikacji. Nie jest natomiast możliwe zażądanie przez aplikację dostępu do dodatkowych możliwości systemu czy podniesienie uprawnień w czasie kiedy jest ona w stanie wykonywana.

Zaletami wykorzystywania kontenerów aplikacji są:

- Redukcja obszaru ataków
Aplikacje otrzymują tylko możliwości jakie zostały zadeklarowane w kodzie i są wymagane do ich uruchomienia.
- Kontrola i zgoda użytkownika
Informacje o możliwym wykorzystaniu informacji poufnych są automatycznie publikowane w Sklepie, w sekcji szczegóły dotyczące aplikacji.

- Izolacja
Aplikacje działające w ramach Windows Phone są odizolowane od siebie. Komunikacja między aplikacjami jest ściśle kontrolowana i odbywa się za pomocą przygotowanych kanałów komunikacji i określonych typów danych.

Wykorzystując kontenery aplikacji i przydzielając minimalne wymagane uprawnienia potrzebne do uruchomienia każdej aplikacji, ogranicza się możliwość przenikania złośliwego oprogramowania do innych kontenerów. W sytuacji kiedy aplikacja w jednym kontenerze zostanie skompromitowana mechanizm izolacji procesów między kontenerami utrzyma złośliwe oprogramowanie tylko w tym kontenerze. Reszta systemu będzie bezpieczna.

6.2.6 Ochrona aplikacji systemu operacyjnego

Firma Microsoft dba o to żeby system operacyjny był bezpieczny i odporny na ataki. Jednakże aplikacje pisane do pracy w Windows Phone mogą stanowić potencjalne zagrożenie dla bezpieczeństwa całego systemu. Powodem tego jest to iż złośliwe oprogramowanie bazuje na tym, że aplikacje pisane są przez ludzi i mogą zawierać luki, które mogą zostać wykorzystane do nieautoryzowanego dostępu do systemu. Windows Phone zawiera usprawnienia zapobiegające i utrudniające wykonywanie ataków niskiego poziomu takich jak np. przepełnienie bufora. Mechanizmy ASLR (Address space layout randomization) i DEP (Data execution prevention) redukują i ograniczają możliwość wykonywania złośliwego oprogramowania.

Funkcja losowego generowania układu przestrzeni adresowej (ASLR)

Sposobami na osiągnięcie nieautoryzowanego dostępu do systemu są:

- zlokalizowanie luki w uprzywilejowanym procesie uruchomionym w systemie,
- zlokalizowanie w miejscu w pamięci gdzie przechowywany jest ważny kod systemu, podmiana informacji znajdujących się w pamięci.

Wcześniejsze wersje systemów Windows pozwalały aplikacjom na bezpośredni zapis danych do pamięci. Windows Phone stosując kontenery aplikacji ogranicza możliwość komunikacji między aplikacjami. Dzięki temu ogranicza się możliwość dostępu przez złośliwe oprogramowanie do krytycznych obszarów systemu operacyjnego.

Zapobieganie wykonywaniu danych (DEP)

Niechciane oprogramowanie bazuje na możliwości podmiany informacji znajdujących się w pamięci urządzenia z założeniem, że uda się uruchomić podmieniany kod w późniejszym czasie. Mechanizm DEP ogranicza zakres pamięci jaki może zostać wykorzystany przez złośliwe oprogramowanie. Używany jest do tego bit eXecute Never (XN) w procesorze ARM, w który jest wyposażony każdy telefon z Windows Phone. Mechanizm polega na oznaczeniu obszaru pamięci jako tylko do przechowywania informacji, bez możliwości wykonania kodu. Nawet w przypadku pomyślnego załadowania podmienionego kodu do pamięci nie zostanie on uruchomiony.

6.2.7 Aplikacje biznesowe

Każde przedsiębiorstwo może otrzymać od firmy Microsoft narzędzia pozwalające na tworzenie, podpisywanie i publikowanie własnych aplikacji dla systemu Windows Phone. Struktura aplikacji jest taka sama jak aplikacji publikowanych w ramach Sklepu. Różnica polega na sposobie dystrybucji i zakresie przeznaczenia aplikacji. Aplikacje dostarczone przez przedsiębiorstwo mogą zostać wdrożone za pomocą systemu MDM lub innych narzędzi. Aplikacje takie przeznaczone są dla prywatnego użytku.

6.2.8 Portal firmy

Wiele systemów zarządzania urządzeniami mobilnymi (MDM) np. Microsoft System Center 2012 R2 i Windows Intune posiada panel zwany portalem firmy. Za pomocą tej aplikacji można dokonywać zmian i wdrażać własne polityki zabezpieczeń. Jedną z funkcji jest dystrybucja aplikacji dla telefonów. System MDM pozwala na ograniczenie użytkownikowi instalowania aplikacji. Zapobiega to możliwości instalacji aplikacji, które mogą zawierać złośliwe oprogramowanie. Za pomocą portalu firmy można zdefiniować dozwolone aplikacje i pozwolić tylko na ich instalację.

6.2.9 Internet Explorer

Aplikacja Internet Explorer w Windows Phone dba o bezpieczeństwo użytkownika i jego informacji w trakcie przeglądania sieci Internet. Używa w tym celu kontenery aplikacji, które zabezpieczają system operacyjny przed możliwością ataku w przypadku skompromitowania samej przeglądarki internetowej. Dodatkowymi zabezpieczeniami w Internet Explorer są:

- filtr SmartScreen URL Reputation, który blokuje lub ostrzega użytkowników o niebezpiecznych witrynach internetowych,
- szyfrowanie komunikacji za pomocą protokołu SSL,
- przeglądanie stron internetowych bez używania dodatków (plug-ins), które mogą potencjalnie być używane jako nośnik dla złośliwego oprogramowania.

6.3 Kontrola dostępu

Weryfikacja użytkownika jest podstawą prawidłowego zabezpieczenia dostępu do danych. Dostęp może odbywać się na dwa sposoby:

- bezpośrednio – osoba uprawniona może korzystać z danych zgromadzonych w urządzeniu,
- pośrednio – osoba uprawniona korzysta z zaufanych urządzeń, które bezpośrednio dają dostęp do zasobów.

Istnieje wiele technologii, które umożliwiają uwierzytelnianie i autoryzację użytkowników w środowisku Windows Phone dla poniższych scenariuszy:

- dostęp do urządzenia,
- przypisany dostęp,
- listy dozwolonych i zabronionych aplikacji,
- wirtualne karty inteligentne,
- uwierzytelnianie za pomocą certyfikatów,
- połączenia VPN,
- dostęp bezprzewodowy,
- pomoc zdalna.

6.3.1 Dostęp do urządzenia

Główną różnicą pomiędzy systemami Windows Phone 8.1 i Windows 8.1 przeznaczonego dla urządzeń takich jak komputery stacjonarne, laptopy, tablety jest dostęp do urządzenia. Windows 8.1 przeznaczony jest do pracy z wieloma użytkownikami. Weryfikacja użytkownika odbywa się za pomocą danych logowania a każdy z użytkowników posiada swój profil, w którym przechowywane są jego dane.

W urządzeniach z systemem Windows Phone dostęp do urządzenia odbywa się za pomocą kodu PIN. Po prawidłowej weryfikacji kodu PIN użytkownik dostaje dostęp do urządzenia i do wszystkich informacji znajdujących się na nim.

Używając systemu MDM można podnieść poziom bezpieczeństwa np. wymuszając żeby oprócz kody PIN wymagane było używanie hasła dostępu do urządzenia. Dodatkowo zasady bezpieczeństwa przedsiębiorstwa mogą definiować określone wymagania co do długości, złożoności, niepowtarzalności oraz innych ustawień hasła.

Windows Phone dostarcza również poniższe metody ochrony kontroli dostępu do urządzenia:

- Zdalne zablokowanie telefonu
Dział wsparcia może za pomocą systemu MDM zdalnie zablokować urządzenie. Funkcjonalność ta jest przydatna, kiedy urządzenie zostało pozostawione bez kontroli i nie ma do niego fizycznego dostępu. Odblokowanie urządzenia odbywa się za pomocą kodu przesłanego z systemu MDM.
- Zdalna zmiana kodu PIN
Dział wsparcia może za pomocą systemu MDM zdalnie zmienić kod PIN w urządzeniu. Jest to przydatne w sytuacji kiedy użytkownik zapomniał kodu PIN.
- Zdalne wywołanie dzwonka urządzenia
W przypadku zagubienia telefonu jest możliwość zdalnego wywołania dźwięku dzwonka w celu łatwiejszej lokalizacji urządzenia.
- Zdalne wymazanie zawartości urządzenia
Dział wsparcia przedsiębiorstwa może dokonać za pomocą systemu MDM zdalnego wymazania danych na urządzeniu. Funkcjonalność ta jest bardzo przydatna w przypadku zagubienia urządzenia lub jego kradzieży.
- Zdalne wycofanie urządzenia z użytku
System MDM wspiera proces wymiany urządzeń w ramach przedsiębiorstwa. W przypadku kiedy urządzenie zostaje wycofane z użytku w ramach przedsiębiorstwa dokonywane jest zdalne wykasowanie wszystkich danych organizacji jakie były przechowywane w ramach urządzenia. Nie oznacza to wykasowania wszystkich danych przechowywanych na nim. Dane osobiste użytkownika zostają nienaruszone. Funkcjonalność ta jest przydatna w sytuacji kiedy użytkownik używał prywatnego urządzenia do pracy w ramach organizacji. Po wycofaniu urządzenia, użytkownik może nadal go używać do celów domowych.

W celu zabezpieczenia danych przechowywanych na urządzeniu przed próbą zgadnięcia hasła dostępu, Windows Phone zezwala na stosowanie zasady bezpieczeństwa która wymazuje dane urządzenia po określonych nieudanych próbach podania hasła dostępu.

6.3.2 Przypisany dostęp

W celu podniesienia bezpieczeństwa Windows Phone wyposażony jest w funkcję kontrolującą dostęp do aplikacji i funkcji urządzenia. Za pomocą funkcji Przypisany dostęp jest możliwe określenie poziomu dostępu na jaki zezwalamy użytkownikowi. Na przykład można określić jakie aplikacje i funkcje są dozwolone dla użytkownika, a pozostałe zostaną zablokowane. Ograniczenia mogą dotyczyć aplikacji dostarczanych przez systemy MDM w ramach przedsiębiorstwa jak również wbudowanych funkcji i aplikacji. Stosując tę funkcjonalność ograniczamy możliwość instalacji i uruchamiania aplikacji potencjalnie zawierających złośliwe oprogramowanie. Oprócz dostępu do aplikacji Przypisany dostęp pozwala na definiowanie dostępu do wbudowanego wyposażenia urządzenia takiego jak np. aparat, karta pamięci.

6.3.3 Listy dozwolonych i zabronionych aplikacji

W ramach systemu MDM można tworzyć listy dozwolonych i zabronionych aplikacji, które będą dostępne dla użytkownika. Listy te współdziałając z opisaną wcześniej funkcją Przypisany dostęp pozwalają podnieść poziom bezpieczeństwa urządzenia. Na przykład wykorzystując go do zablokowania dostępu do aplikacji Sklep można wymusić aby użytkownicy używali wyłącznie tylko Portalu firmy do instalacji aplikacji. Natomiast w ramach portalu firmy który jest częścią systemu MDM można stworzyć listy dozwolonych aplikacji biznesowych.

Mając na uwadze współdziałanie Listy dostępnych aplikacji z opcją Przydziału dostępu trzeba pamiętać o potencjalnym wystąpieniu konfliktów wynikających z konfiguracji obu funkcji.

6.3.4 Wirtualne karty inteligentne

System Windows Phone 8.1 wspiera wirtualne karty inteligentne. Mają one takie same zastosowanie jak fizyczne karty inteligentne. Różnica między nimi polega na tym, że karty wirtualne używają procesora TPM do przechowywania certyfikatów i skrótów kryptograficznych.

Za pomocą wirtualnych kart inteligentnych może odbywać się uwierzytelnianie dwustopniowe jak i podpisywanie wiadomości e-mail za pomocą protokołu S/MIME.

6.3.5 Uwierzytelnianie za pomocą certyfikatów

W celu podniesienia poziomu bezpieczeństwa wymiany informacji takich jak wiadomości e-mail, jak i dla zabezpieczenia połączeń zdalnych system Windows Phone został wyposażony o wsparcie dla używania certyfikatów. Windows Phone używa protokołu Simple Certificate Enrollment Protocol (SCEP) do zarządzania certyfikatami. Certyfikaty mogą być wykorzystywane w:

- połączeniach bezprzewodowych Wi-Fi (Windows Phone wspiera protokoły EAP-TLS i EAP TTLS jako protokoły uwierzytelniania dla połączeń Wi-Fi),
- wirtualnych kartach inteligentnych (Windows Phone używa wirtualnych kart inteligentnych dla podniesienia bezpieczeństwa przeglądania witryn internetowych jak i do podpisywania i szyfrowania wiadomości e-mail),
- podpisywaniu za pomocą S/MIME (protokół S/MIME wymaga certyfikatów lub wirtualnych kart inteligentnych w celu podpisania wiadomości e-mail).

Certyfikaty są przechowywane w procesorze TPM, w który jest wyposażone każde urządzenie posiadające system Windows Phone. Za pomocą systemu MDM dział wsparcia przedsiębiorstwa może zarządzać certyfikatami przechowywanymi na urządzeniach.

6.3.6 Połączenia VPN

Urządzenia z Windows Phone 8.1 umożliwiają zdalny dostęp dla użytkowników za pomocą wirtualnych sieci prywatnych VPN (Virtual Private Network). Wspierane są oprócz Microsoft również technologie innych różnych producentów np. Check Point, F5, Juniper czy SonicWall.

Urządzenia z Windows Phone 8.1 zapewniają ochronę połączeń VPN za pomocą protokołów IKEv2, IPsec oraz SSL. W przypadku gdy przedsiębiorstwo używa rozwiązań VPN-SSL dostarczonych przez firmy trzecie, w celu zapewnienia kompatybilności z Windows Phone należy pobrać dodatek producenta zapewniający wsparcie VPN-SSL dla Windows Phone.

Wykorzystując system MDM można zapewnić wdrożenia profili połączeń VPN dla użytkowników z jednoczesną konfiguracją ustawień zabezpieczeń.

6.3.7 Dostęp bezprzewodowy

W celu pełnego wykorzystania możliwości oferowanych przez współczesne telefony konieczne jest posiadanie stałego dostępu do sieci Internet. Zapewnia to w ramach sieci komórkowych funkcja transmisji danych. Mimo stałego rozwoju tych sieci nie są one jednak w stanie zapewnić takich parametrów jak sieci bezprzewodowe (Wi-Fi). Dlatego też użytkownicy preferują używanie sieci Wi-Fi zamiast transmisji danych w ramach sieci komórkowych. Połączenia bezprzewodowe również często są wykorzystywane w ramach przedsiębiorstw jak i poza nimi. Bardzo ważnym aspektem w ramach komunikacji za pomocą sieci bezprzewodowych jest bezpieczeństwo.

Windows Phone 8.1 zabezpiecza dostęp do połączeń bezprzewodowe za pomocą protokołów WPA, WPA2 oraz WEP. Od systemu Windows Phone 8.1 dostępne jest również wsparcie dla zabezpieczeń sieci Wi-Fi za pomocą rozwiązań dedykowanych przedsiębiorstwom (EAP-TLS oraz EAP-TTLS). Obydwa protokoły wymagają aby certyfikat klienta był zainstalowany na urządzeniu. Jest on każdorazowo wykorzystywany w procesie uwierzytelniania w sieciach Wi-Fi przedsiębiorstwa. Ważność certyfikatu jest weryfikowana z centrum certyfikacji przedsiębiorstwa.

Wprowadzenie możliwości uwierzytelniania w sieciach Wi-Fi za pomocą certyfikatów protokołów EAP-TLS i EAP-TTLS znacząco podnosi poziom bezpieczeństwa.

Używając systemu MDM istnieje możliwość centralnego zarządzania i przydzielania certyfikatów dla urządzeń. Dodatkowo system MDM zapewnia zasady zabezpieczeń dotyczące sieci bezprzewodowych, takie jak:

- przygotowanie profili znanych i bezpiecznych sieci Wi-Fi, nawet w przypadku kiedy identyfikator sieci (SSID) nie jest rozgłaszany publicznie,
- zabronienie używania urządzenia jak punkt dostępowy hotspot,
- zabronienie użytkownikom dodawania profili sieci Wi-fi i łączenia z niezaufanymi punktami dostępowymi hotspot,
- zabronienie użytkownikom przekierowywania ruchu sieciowego przez połączenia bezprzewodowe (Wi-Fi offloading).

6.3.8 Pomoc zdalna

Windows Phone 8.1 mając na celu wsparcie dla użytkowników rzadko pojawiających się w biurach przedsiębiorstwa posiada funkcjonalność pomocy zdalnej. Pozwala ona na zdalne, bezpieczne połączenie się z urządzeniem przez pracownika działu wsparcia i dokonania niezbędnych czynności w celu usunięcia problemu z urządzeniem lub zainstalowanymi na nim aplikacjami.

7. Wycofanie urządzenia z użytku

Ostatnią fazą cyklu życia urządzenia w ramach przedsiębiorstwa jest jego wycofanie z użytkowania. Zaprzeszanie używania telefonu nie zawsze oznacza koniec jego działania. Część z urządzeń zostaje przekazana w inne ręce a urządzenia które są prywatną własnością użytkowników pozostają w ich posiadaniu. Niezależnie od dalszego przeznaczenia danego urządzenia konieczne jest usunięcie z niego danych i aplikacji organizacji. Usunięciu powinny podlegać poniższe dane, aplikacje oraz ustawienia:

- konta e-mail,
- certyfikaty przedsiębiorstwa,
- profile sieci,
- wdrożone aplikacje przedsiębiorstwa,
- dane powiązane z aplikacjami przedsiębiorstwa,
- zasady zabezpieczeń dotyczące urządzeń mobilnych.

W sytuacji, kiedy użytkownik używał prywatnego urządzenia do pracy w ramach przedsiębiorstwa, koniecznym jest zadbanie o to żeby podczas procesu usuwania danych przedsiębiorstwa nie wykasować prywatnych danych użytkownika.

Szczególnym przypadkiem, kiedy wymagane jest wycofanie urządzenia z użytku jest jego kradzież lub zagubienie. W przypadku braku fizycznego dostępu do urządzenia przez osoby upoważnione wymagane jest wykonanie zdalnego wymazania danych organizacji przechowywanych w urządzeniu.

Używając systemów MDM można zdalnie przeprowadzić proces wymazania danych. W celu uniknięcia możliwości nieautoryzowanego usunięcia powiązania urządzenia z systemem MDM zostały wprowadzone dwie zasady:

- zabronić użytkownikowi ręcznego usunięcia powiązania z systemem MDM,
- zabronić użytkownikowi ręcznego resetowania urządzenia oraz aplikacji MDM.

7.1 Bezpieczne usuwanie danych

Jedną z końcowych faz w ramach wycofania urządzenia z użytku, mających ścisły związek z bezpieczeństwem danych przechowywanych na urządzeniu jest ich bezpieczne i trwałe usunięcie zarówno z pamięci wewnętrznej jak i nośników zewnętrznych (np. karty SD). Należy pamiętać, że przywrócenie urządzenia do ustawień fabrycznych nie kasuje danych z telefonu, a jedynie oznacza zajęte obszary dysku jako wolne, co umożliwia ich późniejsze nadpisanie. Może to powodować złudne wrażenie wykasowania danych z urządzenia podczas kiedy są one tam dalej przechowywane.

W celu skutecznego usunięcia danych należy wykorzystać dedykowane aplikacje do bezpiecznego wymazywania danych.

7.2 Przywracanie ustawień fabrycznych

Przywracanie telefonu z systemem Windows Phone do ustawień fabrycznych powoduje, że zostanie on odtworzony do tego samego stanu, w jakim znajdował się, gdy został włączony po raz pierwszy. Resetowanie telefonu powoduje wymazanie całej zapisanej na nim zawartości, łącznie z grami

i aplikacjami (w tym z informacjami o postępie w grach, danymi aplikacji, wiadomościami SMS, historią połączeń, muzyką, zdjęciami i innymi danymi). Proces resetowania trwa kilka minut.

Resetowanie może być wykonane z poziomu ustawień telefonu lub w przypadku braku interakcji z urządzeniem poprzez odpowiednią kombinację klawiszy.

7.2.1 Resetowanie urządzenia z poziomu ustawień telefonu

Przywrócenie ustawień fabrycznych z poziomu ustawień telefonu można wykonać w ramach opcji Informacje (pkt. 4.1.37).

7.2.2 Resetowanie urządzenia za pomocą przycisków sprzętowych

Jeśli telefon nie reaguje lub nie można przejść do opcji Ustawienia należy zresetować telefon przy użyciu przycisków sprzętowych. W celu przywrócenia ustawień fabrycznych za pomocą przycisków telefonu należy wykonać poniższe kroki:

1. Wyłączyć zasilanie.
2. Nacisnąć i przytrzymać przycisk REGULACJA GŁOŚNOŚCI W DÓŁ i krótko przycisk ZASILANIE.
3. Po wyświetleniu ikony na ekranie zwolnić przycisk REGULACJA GŁOŚNOŚCI W DÓŁ
4. Po pojawieniu się wykrzyknika należy nacisnąć przyciski sprzętowe w następującej kolejności:

REGULACJA GŁOŚNOŚCI W GÓRĘ > REGULACJA GŁOŚNOŚCI W DÓŁ > ZASILANIE >
REGULACJA GŁOŚNOŚCI W DÓŁ.

8. Spis rysunków

Rys. 1 Fazy cyklu życia platformy Windows Phone	9
Rys. 2 Okno Wybierz język	17
Rys. 3 Okno Zaczynamy i Warunki użytkowania	18
Rys. 4 Okno Połącz z Wi-Fi	18
Rys. 5 Okno konfiguracji Czujnik Wi-Fi	19
Rys. 6 Okno wyboru ustawień telefonu – zalecane / dostosuj	20
Rys. 7 Okno niestandardowej konfiguracji urządzenia	20
Rys. 8 Okno wyboru ustawień Czas i region	21
Rys. 9 Okno połączenia urządzenia z kontem Microsoft.....	21
Rys. 10 Okna finalizacji ustawień.....	21
Rys. 11 Ustawienia systemu Windows Phone	23
Rys. 12 Opcje ustawień Ekran + motyw	24
Rys. 13 Opcje ustawień Dzwonki + dźwięki	24
Rys. 14 Opcje ustawień Poczta + konta	25
Rys. 15 Opcje ustawień Ekran blokady	27
Rys. 16 Opcje ustawień Dzwonki + dźwięki	28
Rys. 17 Opcje ustawień Wi-Fi i Czujnik sieci Wi-Fi	29
Rys. 18 Opcje ustawień Tryb samolotowy	30
Rys. 19 Opcje ustawień Bluetooth	31
Rys. 20 Opcje ustawień Komórkowe + SIM	32
Rys. 21 Opcje ustawień NFC	33
Rys. 22 Udostępnienie połączenia Internetowego.....	34
Rys. 23 Konfiguracja połączenia VPN	35
Rys. 24 Kącik z aplikacjami.....	36
Rys. 25 Ustawienie opcji Praca	37
Rys. 26 Ustawienie opcji Kącik dziecięcy	38
Rys. 27 Opcje ustawień Oszczędzanie baterii	38
Rys. 28 Opcje ustawień Czujnik danych	39
Rys. 29 Opcje ustawień Czujnik pamięci	39
Rys. 30 Opcje ustawień Jasność	40
Rys. 31 Opcje ustawień Obrót ekranu	40
Rys. 32 Opcje ustawień Wyświetl mój ekran	41
Rys. 33 Opcje ustawień Znajdź mój telefon	41
Rys. 34 Opcje ustawień Kopia zapasowa	42
Rys. 35 Opcje ustawień Synchronizacja ustawień	43
Rys. 36 Opcje ustawień Tryb samochodowy	44
Rys. 37 Opcje ustawień Lokalizacja	45
Rys. 38 Opcje ustawień Reklamy	46
Rys. 39 Opcje ustawień Data + godzina	46
Rys. 40 Opcje ustawień Klawiatura	47
Rys. 41 Opcje ustawień Język	48
Rys. 42 Opcje ustawień Region	48

Rys. 43 Opcje ustawień Raport	50
Rys. 44 Opcje ustawień Mowa	50
Rys. 45 Opcje ustawień Ułatwienia dostępu	53
Rys. 46 Opcje ustawień Aplikacje dla akcesoriów	54
Rys. 47 Opcje ustawień Aktualizacje	54
Rys. 48 Opcje ustawień Informacje	55
Rys. 49 Opcje ustawień Konto Nokia	56
Rys. 50 Opcje ustawień Punkt dostępu	57
Rys. 51 Opcje ustawień Audio	57
Rys. 52 Opcje ustawień Dotknij	58
Rys. 53 Opcje ustawień Kontrola pamięci	58
Rys. 54 Opcje ustawień Filtr połączeń + SMS	59
Rys. 55 Opcje ustawień Ekran podglądu	60
Rys. 56 Opcje ustawień opcji Wyświetl	60
Rys. 57 Opcje ustawień sieć +	61
Rys. 58 Opcja info + dodatki	61
Rys. 59 Opcje ustawień Koncentrator urządzeń	62
Rys. 60 Ustawienia opcji Oceń nas	63
Rys. 61 Ustawienia z podziałem na aplikacje.....	64
Rys. 62 Ustawienia Internet Explorer	64
Rys. 63 Ustawienia Internet Explorer - wybór wersji.....	65
Rys. 64 Ustawienia Internet Explorer - przycisk na pasku adresu.....	66
Rys. 65 Ustawienia Internet Explorer - czujnik danych.....	66
Rys. 66 Ustawienia Internet Explorer - usuwanie historii.....	67
Rys. 67 Ustawienia zawansowane Internet Explorer	68
Rys. 68 Ustawienia zawansowane Internet Explorer - styl widoku czytania.....	68
Rys. 69 Ustawienia zawansowane Internet Explorer - pliki cookie z witryn.....	69
Rys. 70 Ustawienia zawansowane Internet Explorer - hasła do witryn.....	69
Rys. 71 Ustawienia zawansowane Internet Explorer - domyślny dostawca wyszukiwania.....	69
Rys. 72 Ustawienia zawansowane Internet Explorer - zarządzanie pamięcią w urządzeniu.....	70
Rys. 73 Ustawienia opcji Kontakty	71
Rys. 74 Ustawienia aplikacji Mapy	72
Rys. 75 Ustawienia aktualizacji aplikacji Mapy	72
Rys. 76 Ustawienia aplikacji Office	73
Rys. 77 Ustawienia aplikacji Portfel	74
Rys. 78 Włączenie i wyłączenie używania lokalizacji w aplikacji Sklep	75
Rys. 79 Ustawienia spersonalizowanych propozycji w ramach aplikacji Sklep	75
Rys. 80 Włączenie automatycznych aktualizacji aplikacji.....	76
Rys. 81 Uruchomienie automatycznych aktualizacji aplikacji.....	76
Rys. 82 Ustawienia aplikacji Sklep	76
Rys. 83 Ustawienia opcji Telefon	78
Rys. 84 Ustawienia Wiadomości	79
Rys. 85 Ustawienia opcji Wyszukiwania	81
Rys. 86 Ustawienia opcji Zdjęcia + aparat	82

