MC

Tłumaczenie standardów i rekomendacji
w zakresie cyberbezpieczeństwa

Bezpieczeństwo urządzeń mobilnych:

Organizacyjne urządzenia mobilne obsługiwane osobiście przez użytkowników (COPE)

NIST SP 1800-21_wer. 1.0_PL

NIST SP 1800-21_PL

26 września 2024

Bezpieczeństwo urządzeń mobilnych: Organizacyjne urządzenia mobilne obsługiwane osobiście przez użytkowników (COPE)

Zawiera: Streszczenie (A); Podejście, architektura i charakterystyka bezpieczeństwa (B); oraz Poradniki „how-to” (C)

Publikacja dostępna pod adresem:

Rekomendacje cyberbezpieczeństwa

NIST SPECIAL PUBLICATION 1800-21

Mobile Device Security:

Corporate-Owned Personally-Enabled (COPE)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Joshua M. Franklin*
Gema Howell
Kaitlin Boeckl
Naomi Lefkovitz
Ellen Nadeau*
Dr. Behnam Shariati
Jason G. Ajmo
Christopher J. Brown
Spike E. Dog
Frank Javar
Michael Peck
Kenneth F. Sandlin

*Former employee; all work for this publication done while at employer.

Final

This publication is available free of charge from:

https://doi.org/10.6028/NIST.SP.1800-21

NIST SPECIAL PUBLICATION 1800-21

Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Joshua M. Franklin*
Gema Howell
Kaitlin Boeckl
Naomi Lefkovitz
Ellen Nadeau*
Applied Cybersecurity Division
Information Technology Laboratory

Dr. Behnam Shariati
University of Maryland, Baltimore County
Department of Computer Science and Electrical Engineering
Baltimore, Maryland

Jason G. Ajmo
Christopher J. Brown
Spike E. Dog
Frank Javar
Michael Peck
Kenneth F. Sandlin
The MITRE Corporation
McLean, Virginia

**Former employee; all work for this publication done while at employer.*

Final

September 2020

U.S. Department of Commerce

Wilbur Ross, Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

O PUBLIKACJI

Niniejsze opracowanie **NIST SP 1800-21_PL wer. 1.0, *Bezpieczeństwo urządzeń mobilnych: Organizacyjne urządzenia mobilne obsługiwane osobiście przez użytkowników (COPE)***, stanowi tłumaczenie publikacji NIST SP 1800-21, *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)*, i zostało opracowane za zgodą National Institute of Science and Technology.

Przytaczane i cytowane w publikacji przepisy, okólniki, rozporządzenia wykonawcze, dyrektywy, normy, standardy, polityki, memoranda itp. odnoszą się, o ile nie zaznaczono inaczej, do prawodawstwa i rynku amerykańskiego. Jeżeli cytowany fragment ma przełożenie lub odpowiednik w polskim porządku prawnym lub normalizacyjnym, wówczas informacje te wskazane są bezpośrednio w tekście lub w przypisach.

W publikacji posłużono się pojęciami zdefiniowanymi w oryginalnej (angielskiej) wersji dokumentu, na podstawie którego powstały niniejsze zalecenia.

Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim. Pozostałe role i funkcje zostały przedstawione w języku angielskim[1]. Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.

Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa***.

Podmioty, urządzenia lub materiały o charakterze komercyjnym prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie. Taka identyfikacja nie stanowi rekomendacji, poparcia ani nie ma na celu sugerowania, że dane podmioty, materiały lub urządzenia są bezwzględnie najlepsze z dostępnych dla osiągnięcia danego celu

[1] Kluczowi uczestnicy zarządzania ryzykiem – patrz: Narodowe Standardy Cyberbezpieczeństwa

SPIS TREŚCI

NIST SP 1800-21_PL **1**

O PUBLIKACJI **4**

SPIS TREŚCI **5**

SPIS ILUSTRACJI **13**

SPIS TABEL **21**

NIST SP 1800-21A_PL **22**

STRESZCZENIE **24**

WYZWANIE **25**

ROZWIĄZANIE **25**

KORZYŚCI **27**

DZIELENIE SIĘ OPINIAMI **28**

PARTNERZY/WSPÓLNICY W ZAKRESIE TECHNOLOGII **28**

NIST SP 1800-21B_PL **30**

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE **32**

PRZEWODNIKI NIST DOTYCZĄCE PRAKTYK W ZAKRESIE CYBERBEZPIECZEŃSTWA **32**

STRESZCZENIE **33**

SŁOWA KLUCZOWE **34**

1. PODSUMOWANIE **36**

1.1. WYZWANIE 37

1.2. ROZWIĄZANIE 38

1.2.1. Normy i wytyczne *40*

1.3. KORZYŚCI 40

2. SPOSÓB KORZYSTANIA Z NINIEJSZEGO PRZEWODNIKA **42**

2.1. KONWENCJE TYPOGRAFICZNE 44

3. PODEJŚCIE **45**

3.1. ODBIORCY 45

3.2. ZAKRES 46

3.2.1. Orvilia Development *47*

3.3. ZAŁOŻENIA 50

3.3.1. Inżynieria systemów *51*

3.4. SZACOWANIE RYZYKA 52

3.4.1. Szacowanie ryzyka w fikcyjnej organizacji Orvilia Development *53*

3.4.2. Opracowywanie opisów zdarzeń powodujących zagrożenie *54*

Tłumaczenie

3.4.2.1. Zdarzenie powodujące zagrożenie 1 — Nieautoryzowany dostęp do wrażliwych informacji za pośrednictwem złośliwej aplikacji lub aplikacji naruszającej prywatność 56
3.4.2.2. Zdarzenie powodujące zagrożenie 2 — Kradzież danych uwierzytelniających za pośrednictwem usługi krótkich wiadomości tekstowych (ang. Short Message Service – SMS) lub kampanii e-mail służącej do wyłudzania informacji 57
3.4.2.3. Zdarzenie powodujące zagrożenie 3 — Złośliwe aplikacje instalowane za pośrednictwem adresów URL w wiadomościach SMS lub e-mail 58
3.4.2.4. Zdarzenie powodujące zagrożenie 4 — Utrata poufności i integralności w wyniku wykorzystania znanej podatności w systemie operacyjnym lub oprogramowaniu układowym 59
3.4.2.5. Zdarzenie powodujące zagrożenie 5 — Naruszenie prywatności poprzez niewłaściwe wykorzystanie czujników urządzenia 60
3.4.2.6. Zdarzenie powodujące zagrożenie 6 — Naruszenie integralności urządzenia lub jego komunikacji sieciowej poprzez instalację złośliwego systemu EMM/MDM, sieci, profili VPN lub certyfikatów. 61
3.4.2.7. Zdarzenie powodujące zagrożenie 7 — Utrata poufności wrażliwych informacji poprzez podsłuchiwanie niezaszyfrowanej komunikacji urządzenia 62
3.4.2.8. Zdarzenie powodujące zagrożenie 8 — Naruszenie integralności urządzenia poprzez zastosowanie kodu odblokowującego, który został zaobserwowany, wywnioskowany lub pozyskany na drodze ataku siłowego 63
3.4.2.9. **....**Zdarzenie powodujące zagrożenie 9 — Nieautoryzowany dostęp do usług zaplecza poprzez luki w uwierzytelnianiu lub przechowywaniu danych uwierzytelniających w wewnętrznie opracowanych aplikacjach 64
3.4.2.10. Zdarzenie powodujące zagrożenie 10 — Nieautoryzowany dostęp do zasobów przedsiębiorstwa z urządzenia niezarządzanego i narażonego na naruszenie bezpieczeństwa 65
3.4.2.11. Zdarzenie powodujące zagrożenie 11 — Utrata danych organizacji z powodu zgubienia lub kradzieży urządzenia 65
3.4.2.12. Zdarzenie powodujące zagrożenie 11 — Utrata poufności danych organizacji z powodu ich nieautoryzowanego przechowywania w usługach niezarządzanych przez organizację 66
3.4.3. Identyfikacja podatności i warunków predysponujących 67
3.4.4. Podsumowanie wyników szacowania ryzyka 68
3.4.5. Szacowanie ryzyka dla prywatności 70
3.4.5.1. Potencjalne problemy dla osób fizycznych 71
3.4.5.1.1. Działanie na danych 1: Blokowanie dostępu i wymazywanie pamięci urządzeń 71
3.4.5.1.2. Działanie na danych 2: Monitorowanie pracowników 72
3.4.5.1.3. Działanie na danych 3: Udostępnianie danych między stronami 72
3.5. CELE ROZWIĄZANIA 73
3.5.1. Pierwotna architektura 74
3.5.2. Cele bezpieczeństwa 75
3.6. TECHNOLOGIE 76
3.6.1. Komponenty architektury 77
3.6.1.1. Zaufane środowisko wykonawcze 77
3.6.1.2. Zarządzanie mobilnością w przedsiębiorstwie 77
3.6.1.3. Wirtualna sieć prywatna 79
3.6.1.4. Usługa weryfikacji aplikacji mobilnych 80
3.6.1.5. Ochrona przed zagrożeniami mobilnymi 81
3.6.1.6. Analiza zagrożeń mobilnych 82
3.6.1.7. Możliwości mobilnego systemu operacyjnego 82
3.6.1.7.1. Bezpieczny rozruch 82

3.6.1.7.2. Zaświadczanie urządzeń ... 83
3.6.1.7.3. Zarządzanie urządzeniem i interfejs API MDM ... 83

4. ARCHITEKTURA ... 85

4.1. OPIS ARCHITEKTURY ... 87
4.1.1. Integracja w przedsiębiorstwie ... 88
4.1.2. Integracja komponentów mobilnych ... 90
4.1.2.1. Appthority – MobileIron ... 91
4.1.2.2. Lookout – MobileIron ... 91
4.1.2.3. Kryptowire – MobileIron ... 92
4.1.2.4. Palo Alto Networks – MobileIron ... 93
4.1.2.4.1. Zgodność z normą FIPS ... 94
4.1.2.5. Integracja rozwiązania EMM z systemami iOS i Android ... 95
4.2. MAPA DANYCH PRYWATNOŚCI W ARCHITEKTURZE BEZPIECZEŃSTWA PRZEDSIĘBIORSTWA ... 97
4.3. MAPA ŚRODKÓW BEZPIECZEŃSTWA ... 99

5. ANALIZA CHARAKTERYSTYKI BEZPIECZEŃSTWA ... 100

5.1. ZAŁOŻENIA I OGRANICZENIA ANALIZY ... 100
5.2. TESTOWANIE PROJEKTU ... 100
5.2.1. Zdarzenie powodujące zagrożenie 1 (TE1) — Nieautoryzowany dostęp do poufnych informacji za pośrednictwem złośliwej lub naruszającej prywatność aplikacji ... 101
5.2.2. Zdarzenie powodujące zagrożenie 2 (TE-2) — Kradzież danych uwierzytelniających za pośrednictwem kampanii wiadomości SMS lub e-mail służącej do wyłudzania informacji ... 102
5.2.3. Zdarzenie powodujące zagrożenie 3 — Złośliwe aplikacje instalowane za pośrednictwem adresu URL w wiadomościach SMS lub e-mail ... 103
5.2.4. Zdarzenie powodujące zagrożenie 4 — Utrata poufności i integralności w wyniku wykorzystania znanej podatności w systemie operacyjnym lub oprogramowaniu układowym ... 104
5.2.5. Zdarzenie powodujące zagrożenie 5 — Naruszenie prywatności poprzez niewłaściwe wykorzystanie czujników urządzenia ... 105
5.2.6. Zdarzenie powodujące zagrożenie 6 — Naruszenie integralności urządzenia lub jego komunikacji sieciowej poprzez instalację złośliwego systemu EMM/MDM, sieci, profili VPN lub certyfikatów ... 106
5.2.7. Zdarzenie powodujące zagrożenie 7 — Utrata poufności wrażliwych informacji poprzez podsłuchiwanie niezaszyfrowanej komunikacji urządzenia ... 108
5.2.8. Zdarzenie powodujące zagrożenie 8 — Naruszenie integralności urządzenia poprzez zastosowanie kodu odblokowującego, który został zaobserwowany, wywnioskowany lub pozyskany na drodze ataku siłowego ... 109
5.2.9. ...Zdarzenie powodujące zagrożenie 9 — Nieautoryzowany dostęp do usług zaplecza poprzez luki w uwierzytelnianiu lub przechowywaniu danych uwierzytelniających w wewnętrznie opracowanych aplikacjach ... 110
5.2.10. Zdarzenie powodujące zagrożenie 10 — Nieautoryzowany dostęp do zasobów przedsiębiorstwa z urządzenia niezarządzanego i narażonego na naruszenie bezpieczeństwa ... 111
5.2.11. Zdarzenie powodujące zagrożenie 11 — Utrata danych organizacji z powodu zgubienia lub kradzieży urządzenia ... 111

5.2.12. Zdarzenie powodujące zagrożenie 12 — Utrata poufności danych organizacji z powodu ich nieautoryzowanego przechowywania w usługach niezarządzanych przez organizację 113
5.3. SCENARIUSZE I USTALENIA 114
5.3.1. Zestawienie ról roboczych z ram cyberbezpieczeństwa i ram NICE 115
5.3.2. Scenariusze i ustalenia związane ze zdarzeniami powodującymi zagrożenia 115
5.3.3. Scenariusze i ustalenia związane z działaniami na danych 117

6. WNIOSKI 119

7. UWAGI DOTYCZĄCE KOLEJNYCH PROJEKTÓW 120

ZAŁĄCZNIK A AKRONIMY 121

ZAŁĄCZNIK B SŁOWNIK 124

ZAŁĄCZNIK C REFERENCJE 132

ZAŁĄCZNIK D NORMY I WYTYCZNE 141

ZAŁĄCZNIK E REJESTRACJA URZĄDZEŃ MOBILNYCH Z SYSTEMAMI ANDROID, APPLE I SAMSUNG KNOX 144

E.1 URZĄDZENIA Z SYSTEMEM ANDROID 144
E.2 URZĄDZENIA Z SYSTEMEM IOS 144
E.3 URZĄDZENIA Z SYSTEMEM SAMSUNG KNOX 145

ZAŁĄCZNIK F SZACOWANIE RYZYKA 146

F.1 SZACOWANIE RYZYKA 146
F.1.1 Zadanie 1-1: Cel szacowania ryzyka 148
F.1.2 Zadanie 1-2: Zakres szacowania ryzyka 148
F.1.3 Zadanie 1-3: Założenia i ograniczenia szacowania ryzyka 151
F.1.3.1 Założenia szacowania ryzyka 151
F.1.3.2 Ograniczenia szacowania ryzyka 151
F.1.4 Zadanie 1-4: Źródła informacji o zagrożeniach, podatnościach i wpływie na potrzeby szacowania ryzyka 155
F.1.4.1 Źródła informacji o zagrożeniach 155
F.1.4.2 Źródła informacji o podatnościach 156
F.1.4.3 Źródła informacji o skutkach 156
F.1.5 Zadanie 1-5: Określenie modelu ryzyka i podejścia analitycznego na potrzeby szacowania ryzyka . 157
F.1.6 Zadanie 2-1: Identyfikacja i charakterystyka głównych źródeł zagrożeń 157
F.1.7 Zadanie 2-2: Identyfikacja potencjalnych zdarzeń powodujących zagrożenie 158
F.1.7.1 Zdarzenie powodujące zagrożenie 1 (TE-1) — Nieautoryzowany dostęp do wrażliwych informacji za pośrednictwem złośliwej lub naruszającej prywatność aplikacji 159
F.1.7.2 Zdarzenie powodujące zagrożenie 2 — Kradzież danych uwierzytelniających za pośrednictwem kampanii wiadomości SMS lub e-mail służącej do wyłudzania informacji 159
F.1.7.3 Zdarzenie powodujące zagrożenie 3 — Złośliwe aplikacje instalowane za pośrednictwem adresu URL w wiadomościach SMS lub e-mail 160
F.1.7.4 Zdarzenie powodujące zagrożenie 4 — Utrata poufności i integralności w wyniku wykorzystania znanej podatności w systemie operacyjnym lub oprogramowaniu układowym 160
F.1.7.5 Zdarzenie powodujące zagrożenie 5 — Naruszenie prywatności poprzez niewłaściwe wykorzystanie czujników urządzenia 161

F.1.7.6 Zdarzenie powodujące zagrożenie 6 — Naruszenie integralności urządzenia lub jego komunikacji sieciowej poprzez instalację złośliwego systemu EMM/MDM, sieci, profili VPN lub certyfikatów. 161
F.1.7.7 Zdarzenie powodujące zagrożenie 7 — Utrata poufności wrażliwych informacji poprzez podsłuchiwanie niezaszyfrowanej komunikacji urządzenia 162
F.1.7.8 Zdarzenie powodujące zagrożenie 8 — Naruszenie integralności urządzenia poprzez zastosowanie kodu odblokowującego, który został zaobserwowany, wywnioskowany lub pozyskany na drodze ataku siłowego 162
F.1.7.9 **.....**Zdarzenie powodujące zagrożenie 9 — Nieautoryzowany dostęp do usług zaplecza poprzez luki w uwierzytelnianiu lub przechowywaniu danych uwierzytelniających w wewnętrznie opracowanych aplikacjach 163
F.1.7.10 Zdarzenie powodujące zagrożenie 10 — Nieautoryzowany dostęp do zasobów przedsiębiorstwa z urządzenia niezarządzanego i narażonego na naruszenie bezpieczeństwa 163
F.1.7.11 **.....**Zdarzenie powodujące zagrożenie 11 — Utrata danych organizacji z powodu zgubienia lub kradzieży urządzenia 164
F.1.7.12 Zdarzenie powodujące zagrożenie 11 — Utrata poufności danych organizacji z powodu ich nieautoryzowanego przechowywania w usługach niezarządzanych przez organizację 164
F.1.8 Zadanie 2-3: Identyfikacja podatności i warunków predysponujących 164
F.1.9 Zadanie 2-4: Określenie prawdopodobieństwa wystąpienia zagrożenia i prawdopodobieństwa jego negatywnych skutków 166
F.1.10 Zadanie 2-5: Określenie stopnia negatywnych skutków 168
F.1.11 Zadanie 2-6: Określenie ryzyka dla organizacji 171

ZAŁĄCZNIK G SZACOWANIE RYZYKA DLA PRYWATNOŚCI 174

G.1 DZIAŁANIE NA DANYCH 1: BLOKOWANIE DOSTĘPU I WYMAZYWANIE PAMIĘCI URZĄDZEŃ 177
G.1.1 Potencjalne problemy dla osób fizycznych 177
G.1.2 Środki zaradcze 178
G.2 DZIAŁANIE NA DANYCH 2: MONITOROWANIE PRACOWNIKÓW 179
G.2.1 Potencjalne problemy dla osób fizycznych 179
G.2.2 Środki zaradcze 180
G.3 DZIAŁANIE NA DANYCH 3: UDOSTĘPNIANIE DANYCH MIĘDZY STRONAMI 181
G.3.1 Potencjalne problemy dla osób fizycznych 181
G.3.2 Środki zaradcze 182
G.4 ŚRODKI ZARADCZE MAJĄCE ZASTOSOWANIE DO RÓŻNYCH DZIAŁAŃ NA DANYCH 183

ZAŁĄCZNIK H INFORMACJE O TESTACH ZDARZEŃ POWODUJĄCYCH ZAGROŻENIA 185

H.1 ZDARZENIE POWODUJĄCE ZAGROŻENIE 1 (TE-1) — NIEAUTORYZOWANY DOSTĘP DO POUFNYCH INFORMACJI ZA POŚREDNICTWEM ZŁOŚLIWEJ LUB NARUSZAJĄCEJ PRYWATNOŚĆ APLIKACJI 185
H.2 ZDARZENIE POWODUJĄCE ZAGROŻENIE 2 — KRADZIEŻ DANYCH UWIERZYTELNIAJĄCYCH ZA POŚREDNICTWEM USŁUGI SMS LUB KAMPANII E-MAIL SŁUŻĄCEJ DO WYŁUDZANIA INFORMACJI 186
H.3 ZDARZENIE POWODUJĄCE ZAGROŻENIE 3 — ZŁOŚLIWE APLIKACJE INSTALOWANE ZA POŚREDNICTWEM ADRESU URL W WIADOMOŚCIACH SMS LUB E-MAIL 187
H.4 ZDARZENIE POWODUJĄCE ZAGROŻENIE 4 — UTRATA POUFNOŚCI I INTEGRALNOŚCI W WYNIKU WYKORZYSTANIA ZNANEJ PODATNOŚCI W SYSTEMIE OPERACYJNYM LUB OPROGRAMOWANIU UKŁADOWYM 194
H.5 ZDARZENIE POWODUJĄCE ZAGROŻENIE 5 — NARUSZENIE PRYWATNOŚCI POPRZEZ NIEWŁAŚCIWE WYKORZYSTANIE CZUJNIKÓW URZĄDZENIA 196

H.6 Zdarzenie powodujące zagrożenie 6 — Naruszenie integralności urządzenia lub jego komunikacji sieciowej poprzez instalację złośliwego systemu EMM/MDM, sieci, profili VPN lub certyfikatów. 197
H.7 Zdarzenie powodujące zagrożenie 7 — Utrata poufności wrażliwych informacji poprzez podsłuchiwanie niezaszyfrowanej komunikacji urządzenia....204
H.8 Zdarzenie powodujące zagrożenie 8 — Naruszenie integralności urządzenia poprzez zastosowanie kodu odblokowującego, który został zaobserwowany, wywnioskowany lub pozyskany na drodze ataku siłowego....205
H.9 … Zdarzenie powodujące zagrożenie 9 — Nieautoryzowany dostęp do usług zaplecza poprzez luki w uwierzytelnianiu lub przechowywaniu danych uwierzytelniających w wewnętrznie opracowanych aplikacjach 206
H.10 Zdarzenie powodujące zagrożenie 10 — Nieautoryzowany dostęp do zasobów przedsiębiorstwa z urządzenia niezarządzanego i narażonego na naruszenie bezpieczeństwa....207
H.11 Zdarzenie powodujące zagrożenie 11 — Utrata danych organizacji z powodu zgubienia lub kradzieży urządzenia 209
H.12 Zdarzenie powodujące zagrożenie 12 — Utrata poufności danych organizacji z powodu ich nieautoryzowanego przechowywania w usługach niezarządzanych przez organizację 210

ZAŁĄCZNIK I PRZYKŁADOWE ZESTAWIENIE ŚRODKÓW BEZPIECZEŃSTWA....211

NIST SP 1800-21C_PL 235

1. WPROWADZENIE....238

1.1. Struktura przewodnika po praktykach....238
1.2. Omówienie rozwiązania....240
1.3. Konwencje typograficzne....241
1.4. Podsumowanie architektury logicznej....242

2. INSTRUKCJE INSTALOWANIA PRODUKTÓW....243

2.1. Mobile Threat Detection firmy Appthority....243
2.2. EMM+S firmy Kryptowire 243
2.3. Mobile Endpoint Security firmy Lookout....243
2.4. MobileIron Core firmy Mobileron....243
2.4.1. Instalowanie systemu MobileIron Core i Stand-Alone Sentry....244
2.4.2. Ogólna konfiguracja systemu MobileIron Core....244
2.4.3. Aktualizacja systemu MobileIron Core 244
2.4.4. Integracja z usługą Microsoft Active Directory 251
2.4.5. Tworzenie etykiet użytkowników mobilnych....256
2.5. Integracja aplikacji Palo Alto Networks GlobalProtect z systemem MobileIron....258
2.5.1. Konfiguracja systemu MobileIron....259
2.5.1.1. Konfigurowanie protokołu SCEP (ang. Simple Certificate Enrolment Protocol) 259
2.5.1.2. Tworzenie konfiguracji aplikacji Palo Alto Networks GlobalProtect 262
2.5.2. Podstawowa konfiguracja urządzenia Palo Alto Networks....263
2.5.2.1. Konfiguracja interfejsu zarządzania 263
2.5.2.2. 2.5.2.3. Konfigurowanie serwera DNS i protokołu NTP 266
2.5.3. Konfiguracja interfejsów i stref urządzenia Palo Alto Networks 269

Tłumaczenie

2.5.3.1. Tworzenie interfejsów i adresów Ethernet 269
2.5.3.2. Tworzenie stref bezpieczeństwa 273
2.5.4. Konfigurowanie routera *275*
2.5.5. Konfiguracja interfejsu tunelowego *277*
2.5.6. Konfiguracja aplikacji i zasad bezpieczeństwa *278*
2.5.6.1. Konfigurowanie aplikacji 278
2.5.6.2. Konfiguracja zasad bezpieczeństwa 281
2.5.6.2.1. Tworzenie zasad bezpieczeństwa 282
2.5.6.2.2. Wdrożone zasady bezpieczeństwa 286
2.5.7. Translacja adresów sieciowych *288*
2.5.8. Konfiguracja sieci SSL VPN *291*
2.5.8.1. Konfiguracja uwierzytelniania użytkowników końcowych 291
2.5.8.1.1. Konfiguracja profilu serwera 291
2.5.8.1.2. Konfiguracja profilu uwierzytelniania 293
2.5.8.1.3. Konfiguracja identyfikacji użytkownika 295
2.5.8.1.4. Konfiguracja reguły uwierzytelniania 297
2.5.9. Importowanie certyfikatów *300*
2.5.10. Konfigurowanie profilu certyfikatu *303*
2.5.11. Konfigurowanie profilu usługi SSL/TLS *304*
2.5.12. Konfigurowanie filtrowania adresów URL *305*
2.5.13. Konfigurowanie bramy i portalu GlobalProtect *308*
2.5.13.1. Konfigurowanie bramy GlobalProtect 309
2.5.13.2. Konfigurowanie portalu GlobalProtect 314
2.5.14. Konfigurowanie automatycznych aktualizacji zagrożeń i aplikacji *318*
2.6. INTEGRACJA USŁUGI KRYPTOWIRE EMM+S Z SYSTEMEM MOBILEIRON 320
2.6.1. Dodawanie konta w interfejsie API MobileIron dla usługi Kryptowire *321*
2.6.2. Kontakt z Kryptowire w celu utworzenia połączenia przychodzącego *324*
2.7. INTEGRACJA USŁUGI LOOKOUT MOBILE ENDPOINT SECURITY Z SYSTEMEM MOBILEIRON 325
2.7.1. Dodawanie konta w interfejsie API MobileIron dla usługi Lookout *325*
2.7.2. Dodawanie etykiet w systemie MobileIron dla usługi Lookout *329*
2.7.3. .....Dodawanie aplikacji Lookout for Work dla systemu Android do katalogu aplikacji systemu MobileIron *331*
2.7.4. Stosowanie etykiet do aplikacji Lookout for Work dla systemu Android *334*
2.7.5. .Dodawanie aplikacji Lookout for Work dla systemu iOS do katalogu aplikacji systemu MobileIron *337*
2.7.5.1. Importowanie aplikacji Lookout for Work 337
2.7.5.2. Stosowanie etykiet systemu MobileIron do aplikacji Lookout for Work 341
2.7.5.3. Tworzenie pliku konfiguracji zarządzanej aplikacji dla Lookout for Work 343
2.7.5.4. Stosowanie etykiet do konfigurowania aplikacji zarządzanej dla Lookout for Work 345
2.7.6. Dodawanie łącznika MDM dla systemu MobileIron do usługi Lookout MES *347*
2.7.7. Konfigurowanie reakcji systemu MobileIron na ryzyko *352*
2.7.7.1. Dodawanie reguły kontroli aplikacji w systemie MobileIron 352
2.7.7.2. Dodawanie akcji zgodności w systemie MobileIron 354
2.7.7.3. Tworzenie zasady bezpieczeństwa systemu MobileIron dla usługi Lookout MES 356
2.7.7.4. ..... Zastosowanie etykiety usługi Lookout MES do zasady bezpieczeństwa systemu MobileIron 358

Tłumaczenie

2.8. INTEGRACJA USŁUGI APPTHORITY MOBILE THREAT DETECTION Z SYSTEMEM MOBILEIRON.....360
2.8.1. Tworzenie konta API w systemie MobileIron dla łącznika Appthority.....361
2.8.2. Wdrożenie Appthority Connector Open Virtualization Appliance.....364
2.8.3. Uruchomienie skryptu do wdrażania łącznika dla systemu zarządzania mobilnością w przedsiębiorstwie.....364
2.9. REJESTROWANIE URZĄDZEŃ W SYSTEMIE MOBILEIRON CORE.....365
2.9.1. Nadzorowanie i rejestrowanie urządzeń z systemem iOS.....366
2.9.1.1. Resetowanie urządzenia z systemem iOS.....366
2.9.1.1.1. Resetowanie nienadzorowanego urządzenia za pomocą aplikacji Settings.....366
2.9.1.1.2. Resetowanie nadzorowanego urządzenia przy użyciu narzędzia Configurator 2.....370
2.9.1.2. Przełączanie urządzenia z systemem iOS w tryb nadzorowany.....373
2.9.1.3. 2.9.1.3. Rejestracja w systemie MobileIron Core.....381
2.9.2. Aktywacja aplikacji Lookout for Work w systemie iOS.....387
2.9.3. ..... Wgrywanie profilu służbowego na zarządzane przez firmę urządzenia z systemem Android.....390
2.9.3.1. Aktywacja profilu służbowego na urządzeniach zarządzanych przez firmę.....391
2.9.3.2. Rejestracja urządzeń z systemem Android.....392
ZAŁĄCZNIK A LISTA AKRONIMÓW.....403
ZAŁĄCZNIK B SŁOWNIK.....405
ZAŁĄCZNIK C REFERENCJE.....409

Tłumaczenie

SPIS ILUSTRACJI

Rysunek 1-1 Podsumowanie architektury logicznej 242

Rysunek 2-1 Konfiguracja repozytorium systemu MobileIron 245

Rysunek 2-2 Wersja systemu MobileIron Core 246

Rysunek 2-3 Status pobierania systemu MobileIron 247

Rysunek 2-4 Sprawdzanie poprawności danych w bazie danych 247

Rysunek 2-5 Potwierdzenie sprawdzenia poprawności danych w bazie danych 248

Rysunek 2-6 Potwierdzenie rozpoczęcia sprawdzania poprawności danych w bazie danych 248

Rysunek 2-7 Status sprawdzania poprawności danych w bazie danych 249

Rysunek 2-8 Informacja o konieczności ponownego uruchomienia w celu aktualizacji oprogramowania 249

Rysunek 2-9 Potwierdzenie ponownego uruchomienia w celu aktualizacji oprogramowania 250

Rysunek 2-10 Informacja o możliwości zapisania konfiguracji przed ponownym uruchomieniem 250

Rysunek 2-11 Stan aktualizacji 250

Rysunek 2-12 Możliwość aktualizacji do wersji 9.7.0.1 251

Rysunek 2-13 Ustawienia protokołu LDAP 252

Rysunek 2-14 Jednostki organizacyjne protokołu LDAP 252

Rysunek 2-15 Konfiguracja użytkownika protokołu LDAP 252

Rysunek 2-16 Konfiguracja grupy protokołu LDAP 253

Rysunek 2-17 Wybrana grupa LDAP 254

Rysunek 2-18 Zaawansowane opcje LDAP 254

Rysunek 2-19 Testowanie konfiguracji serwera LDAP 255

Rysunek 2-20 Wynik testu serwera LDAP 256

Rysunek 2-21 Etykiety urządzeń w systemie MobileIron 256

Rysunek 2-22 Dodawanie etykiety urządzenia 257

Rysunek 2-23 Dopasowania do etykiety urządzenia 258

Rysunek 2-24 Lista etykiet w systemie MobileIron 258

Rysunek 2-25 Konfiguracja protokołu SCEP w systemie MobileIron 260

Rysunek 2-26 Test konfiguracji certyfikatu SCEP 261

Rysunek 2-27 Test certyfikatu SCEP 261

Rysunek 2-28 Konfiguracja sieci VPN w systemie MobileIron 263

Rysunek 2-29 Włączony interfejs zarządzania Palo Alto Networks 264

Rysunek 2-30 Konfiguracja interfejsu zarządzania 265

Rysunek 2-31 Informacje ogólne o zaporze sieciowej Palo Alto Networks 266

Rysunek 2-32 Konfiguracja usług Palo Alto Networks 267

Rysunek 2-33 Konfiguracja serwera DNS 268

Rysunek 2-34 Konfiguracja serwera NTP 269

Rysunek 2-35 Interfejsy Ethernet 270

Rysunek 2-36 Konfiguracja interfejsu Ethernet 270

Rysunek 2-37 Konfiguracja protokołu IPv4 interfejsu WAN 271

Rysunek 2-38 Konfiguracja adresu IP interfejsu WAN 272

Rysunek 2-39 Ukończona konfiguracja interfejsu WAN 272

Rysunek 2-40 Lista stref bezpieczeństwa 273

Rysunek 2-41 Konfiguracja strefy bezpieczeństwa interfejsu LAN 274

Rysunek 2-42 Konfiguracja routera wirtualnego 276

Rysunek 2-43 Ustawienia ogólne routera wirtualnego 277

Rysunek 2-44 Interfejs tunelowy SSL VPN 278

Rysunek 2-45 Kategorie aplikacji 279

Rysunek 2-46 Konfiguracja aplikacji Palo Alto Networks w systemie MobileIron 280

Rysunek 2-47 Konfiguracja portu aplikacji MobileIron 281

Rysunek 2-48 Konfiguracja reguły zapory sieciowej w systemie MobileIron dla dostępu DMZ 282

Rysunek 2-49 Konfiguracja reguły bezpieczeństwa strefy źródłowej w systemie MobileIron dla dostępu DMZ 283

Rysunek 2-50 Konfiguracja reguły bezpieczeństwa adresu docelowego w systemie MobileIron dla dostępu DMZ 284

Rysunek 2-51 Konfiguracja reguły bezpieczeństwa protokołu aplikacji w systemie MobileIron dla dostępu DMZ 285

Rysunek 2-52 Konfiguracja reguły bezpieczeństwa akcji w systemie MobileIron dla dostępu DMZ 286

Rysunek 2-53 Reguła wychodzących procesów NAT 288

Rysunek 2-54 Konfiguracja oryginalnego pakietu wychodzących procesów NAT 290

Rysunek 2-55 Konfiguracja pakietów translacji wychodzących procesów NAT 291

Rysunek 2-56 Profil LDAP 293

Rysunek 2-57 Profil uwierzytelniania 294

Rysunek 2-58 Zaawansowane ustawienia profilu uwierzytelniania 295

Rysunek 2-59 Mapowanie grupy LDAP 296

Rysunek 2-60 Lista dołączonych grup LDAP 297

Rysunek 2-61 Strefy źródłowe dla zasady uwierzytelniania 298

Rysunek 2-62 Strefy docelowe dla zasady uwierzytelniania 299

Rysunek 2-63 Akcje profilu uwierzytelniania 300

Rysunek 2-64 Importowanie certyfikatu MobileIron 302

Rysunek 2-65 Profil certyfikatu 304

Rysunek 2-66 Profil głównego certyfikatu wewnętrznego 304

Rysunek 2-67 Profil usługi SSL/TLS 305

Rysunek 2-68 Niestandardowa kategoria adresów URL 306

Rysunek 2-69 Profil filtrowania adresów URL 307

Rysunek 2-70 Zasady bezpieczeństwa filtrowania adresów URL 308

Rysunek 2-71 Ogólna konfiguracja bramy GlobalProtect 309

Rysunek 2-72 Konfiguracja uwierzytelniania dla bramy GlobalProtect 310

Rysunek 2-73 Konfiguracja tunelu dla bramy GlobalProtect 311

Rysunek 2-74 Pula adresów IP klienta VPN 311

Rysunek 2-75 Ustawienia klienta VPN 312

Rysunek 2-76 Konfiguracja zastąpienia uwierzytelniania w sieci VPN 312

Rysunek 2-77 Konfiguracja grupy użytkowników sieci VPN 313

Rysunek 2-78 Konfiguracja tunelu dzielonego dla sieci VPN 314

Rysunek 2-79 Konfiguracja portalu GlobalProtect 315

Rysunek 2-80 Konfiguracja protokołu SSL/TLS portalu GlobalProtect 316

Rysunek 2-81 Konfiguracja bramy zewnętrznej GlobalProtect 317

Rysunek 2-82 Konfiguracja agenta portalu GlobalProtect 318

Rysunek 2-83 Łącze do harmonogramu 319

Rysunek 2-84 Harmonogram aktualizacji zagrożeń 320

Rysunek 2-85 Użytkownicy systemu MobileIron 321

Rysunek 2-86 Konfiguracja użytkownika Kryptowire interfejsu API 322

Rysunek 2-87 Lista użytkowników systemu MobileIron 323

Rysunek 2-88 Przypisywanie przestrzeni do użytkownika Kryptowire interfejsu API 323

Rysunek 2-89 Lista urządzeń w portalu Kryptowire 325

Rysunek 2-90 Lista użytkowników systemu MobileIron 326

Rysunek 2-91 Konfiguracja użytkownika Lookout w systemie MobileIron 327

Rysunek 2-92 Konto administratora usługi Lookout w systemie MobileIron 327

Rysunek 2-93 Przypisywanie przestrzeni do konta usługi Lookout 328

Rysunek 2-94 Lista etykiet w systemie MobileIron 329

Rysunek 2-95 Konfiguracja etykiety „MTP - Low Risk” 330

Rysunek 2-96 Katalog aplikacji w systemie MobileIron 331

Rysunek 2-97 Dodawanie aplikacji Lookout for Work do katalogu aplikacji systemu MobileIron 332

Rysunek 2-98 Konfiguracja aplikacji Lookout for Work 333

Rysunek 2-99 Konfiguracja aplikacji Lookout for Work 333

Rysunek 2-100 Konfiguracja aplikacji Lookout for Work dla systemu AWF 334

Rysunek 2-101 Zastosowanie aplikacji Lookout for Work do urządzeń z systemem Android 335

Rysunek 2-102 Okno dialogowe Apply To Labels (Zastosuj do etykiet) 336

Rysunek 2-103 Aplikacja Lookout for Work z zastosowanymi etykietami 336

Rysunek 2-104 Katalog aplikacji w systemie MobileIron 337

Rysunek 2-105 Aplikacja Lookout for Work wybrana ze sklepu iTunes 338

Rysunek 2-106 Konfiguracja aplikacji Lookout for Work 338

Rysunek 2-107 Konfiguracja aplikacji Lookout for Work 339

Rysunek 2-108 Ustawienia zarządzanej aplikacji Lookout for Work 340

Rysunek 2-109 Katalog aplikacji z aplikacją Lookout for Work 340

Rysunek 2-110 Wybrana aplikacja Lookout for Work 341

Rysunek 2-111 Okno dialogowe Apply To Labels (Zastosuj do etykiet) 342

Rysunek 2-112 Katalog aplikacji z aplikacją Lookout for Work 342

Rysunek 2-113 Importowanie konfiguracji aplikacji zarządzanej 344

Rysunek 2-114 Konfiguracja pliku plist 345

Rysunek 2-115 Wybrana konfiguracja aplikacji Lookout 346

Rysunek 2-116 Okno dialogowe Apply To Label (Zastosuj do etykiety) 346

Rysunek 2-117 Konfiguracja aplikacji Lookout z etykietami 347

Rysunek 2-118 Ekran dodawania łącznika do usługi Lookout 348

Rysunek 2-119 Ustawienia łącznika 349

Rysunek 2-120 Ustawienia rejestracji łącznika 350

Rysunek 2-121 Ustawienia synchronizacji łącznika 352

Rysunek 2-122 Reguła kontroli aplikacji w systemie MobileIron 353

Rysunek 2-123 Reguła kontroli aplikacji w systemie MobileIron 354

Rysunek 2-124 Akcja zgodności MTP High Risk 355

Rysunek 2-125 Wybór zasady odniesienia 356

Rysunek 2-126 Akcja zgodności MTP High Risk (MTP — wysokie ryzyko) 357

Rysunek 2-127 Wyzwalacz zasady bezpieczeństwa 358

Rysunek 2-128 Lista zasad 359

Rysunek 2-129 Okno dialogowe Apply To Label (Zastosuj do etykiety) 360

Rysunek 2-130 Ustawienia użytkownika dla usługi Appthority 362

Rysunek 2-131 Użytkownik dla łącznika usługi Appthority 363

Rysunek 2-132 Przypisywanie przestrzeni do łącznika usługi Appthority 363

Rysunek 2-133 Konfiguracja łącznika usługi Appthority w interfejsie wiersza polecenia (*ang. Command Line Interface – CLI*) 365

Rysunek 2-134 Status łącznika usługi Appthority EMM 365

Rysunek 2-135 Ekran resetowania w systemie iOS 367

Rysunek 2-136 Potwierdzenie wymazywania pamięci iPhone'a 368

Rysunek 2-137 Ostateczne potwierdzenie wymazywania pamięci iPhone'a 369

Rysunek 2-138 Wprowadzanie kodu dostępu w systemie iOS 370

Rysunek 2-139 Potwierdzenie zaufania do komputera w systemie iOS 371

Rysunek 2-140 Wprowadzanie kodu dostępu, aby zaufać komputerowi 372

Rysunek 2-141 Potwierdzenie wymazania pamięci w narzędziu Configurator 2 372

Rysunek 2-142 Przywracanie iPhone'a do ustawień fabrycznych 373

Rysunek 2-143 Opcje przygotowania urządzenia 374

Rysunek 2-144 Wybór serwera MDM 375

Rysunek 2-145 Logowanie do konta Apple 375

Rysunek 2-146 Okno dialogowe przypisywania organizacji 376

Rysunek 2-147 Tworzenie organizacji 377

Rysunek 2-148 Konfiguracja tożsamości nadzorującej 378

Rysunek 2-149 Wybór organizacji 378

Rysunek 2-150 Wybór tożsamości nadzorującej 379

Rysunek 2-151 Wybrana organizacja 379

Rysunek 2-152 Konfiguracja tworzenia tożsamości nadzorującej dla Organizacji 380

Rysunek 2-153 Ustawienia asystenta konfiguracji 381

Rysunek 2-154 Oczekiwanie na iPhone'a 381

Rysunek 2-155 Strona rejestracji urządzenia z systemem iOS w systemie MobileIron 382

Rysunek 2-156 Potwierdzenie uruchomienia aplikacji Settings 383

Rysunek 2-157 Instalacja profilu 384

Rysunek 2-158 Instalacja profilu 384

Rysunek 2-159 Ostrzeżenie dotyczące instalacji profilu 385

Rysunek 2-160 Potwierdzenie zaufania do instalowanego profilu 386

Rysunek 2-161 Potwierdzenie instalacji profilu 386

Rysunek 2-162 Ekran startowy aplikacji Lookout for Work 387

Rysunek 2-163 Informacja o uprawnieniach aplikacji Lookout for Work 388

Rysunek 2-164 Monit o uprawnienia do wysyłania powiadomień 388

Rysunek 2-165 Monit o dostęp do lokalizacji 389

Rysunek 2-166 Ekran główny aplikacji Lookout for Work 390

Rysunek 2-167 Konfiguracja protokołu AFW w systemie MobileIron 391

Rysunek 2-168 Konfiguracja systemu AFW 392

Rysunek 2-169 Proces rejestracji w systemie MobileIron 393

Rysunek 2-170 Rejestracja systemu AFW 394

Rysunek 2-171 Instalacja aplikacji MobileIron 394

Rysunek 2-172 Akceptacja regulaminu AFW 395

Rysunek 2-173 Informacje o ochronie prywatności w systemie MobileIron 396

Rysunek 2-174 Powiadomienie o wymaganej konfiguracji systemu MobileIron 397

Rysunek 2-175 Stan urządzenia w systemie MobileIron 398

Rysunek 2-176 Konfiguracja systemu AFW 399

Rysunek 2-177 Tworzenie przestrzeni roboczej w systemie AFW 400

Rysunek 2-178 Preferencje blokady profilu służbowego w systemie MobileIron 400

Rysunek 2-179 Konfiguracja konta Google w systemie MobileIron 401

Rysunek 2-180 Stan urządzenia w systemie MobileIron 402

SPIS TABEL

Tabela 3-1 Zestawienie zdarzeń powodujących zagrożenia z odpowiadającymi im pozycjami w katalogu zagrożeń dla urządzeń mobilnych 55

Tabela 3-2 Identyfikacja podatności i warunków predysponujących 67

Tabela 3-3 Podsumowanie wyników szacowania ryzyka 68

Tabela 4-1 Wykorzystane produkty dostępne na rynku 85

Tabela 5-1 Zestawienie scenariuszy i ustaleń związanych ze zdarzeniami powodującymi zagrożenia 116

Tabela 5-2 Zestawienie scenariuszy i ustaleń związanych z działaniami na danych . 118

Tabela 1-1 Konwencje typograficzne 241

Tabela 2-1 Wdrożone zasady bezpieczeństwa 286

Tabela 2-2 Wdrożone zasady bezpieczeństwa 287

Tabela 2-3 Wdrożone zasady bezpieczeństwa 287

NIST SP 1800-21A_PL

26 września 2024

Bezpieczeństwo urządzeń mobilnych: Organizacyjne urządzenia mobilne obsługiwane osobiście przez użytkowników (COPE)

Tom A
Streszczenie

NIST SPECIAL PUBLICATION 1800-21A

Mobile Device Security:
Corporate-Owned Personally-Enabled (COPE)

Volume A:
Executive Summary

Joshua M. Franklin*
Gema Howell
Kaitlin Boeckl
Naomi Lefkovitz
Ellen Nadeau*
Applied Cybersecurity Division
Information Technology Laboratory

Dr. Behnam Shariati
University of Maryland, Baltimore County
Department of Computer Science and Electrical Engineering
Baltimore, Maryland

Jason G. Ajmo
Christopher J. Brown
Spike E. Dog
Frank Javar
Michael Peck
Kenneth F. Sandlin
The MITRE Corporation
McLean, Virginia

Former employee; all work for this publication done while at employer

September 2020

Final

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-21

STRESZCZENIE

Urządzenia mobilne zapewniają dostęp do istotnych zasobów w miejscu pracy, jednocześnie zapewniając pracownikom elastyczność przy wykonywaniu codziennych czynności. Istnieje kilka opcji wdrożenia urządzeń mobilnych. Jednym z modeli wdrożenia jest udostępnianie pracownikom urządzeń będących własnością firmy[2] (*ang. Corporate-Owned Personally-Enabled – COPE*). Urządzenia COPE są własnością przedsiębiorstwa i są przydzielane pracownikom. Architektury COPE zapewniają elastyczność umożliwiającą zarówno przedsiębiorstwom, jak i pracownikom instalowanie aplikacji na urządzeniach mobilnych należących do przedsiębiorstwa.

Zabezpieczenie urządzeń mobilnych ma kluczowe znaczenie dla ciągłości operacji biznesowych. Urządzenia mobilne mogą zwiększyć wydajność i produktywność, ale mogą również stanowić źródło zagrożenia dla wrażliwych danych. Narzędzia zabezpieczające urządzenia mobilne mogą przeciwdziałać takim zagrożeniom, umożliwiając zabezpieczenie dostępu do sieci i zasobów.

Organizacja National Cybersecurity Center of Excellence (NCCoE) działająca w ramach Narodowego Instytutu Standaryzacji i Technologii (*ang. National Institute of Standards and Technology – NIST*) stworzyła środowisko laboratoryjne w celu badania problemów związanych z zabezpieczaniem urządzeń mobilnych przy jednoczesnym zarządzaniu ryzykiem oraz możliwych sposobów integrowania różnych technologii, aby pomóc organizacjom w zabezpieczeniu ich urządzeń COPE.

W niniejszym przewodniku po praktykach w zakresie cyberbezpieczeństwa NIST (*ang. NIST Cybersecurity Practice Guide*) opisano, w jaki sposób organizacje mogą korzystać ze standardowych produktów dostępnych na rynku, aby zaspokoić swoje potrzeby w zakresie bezpieczeństwa i prywatności urządzeń mobilnych COPE.

[2] Także: organizacja, przedsiębiorstwo, instytucja, jednostka organizacyjna.

WYZWANIE

Urządzenia mobilne są nieodłącznym elementem nowoczesnych miejsc pracy. Pracownicy używają urządzeń COPE do wykonywania zadań, dlatego przed organizacjami stoi wyzwanie polegające na zapewnieniu, aby urządzenia te przetwarzały, modyfikowały i przechowywały wrażliwe dane w bezpieczny sposób. Urządzenia COPE niosą ze sobą specyficzne zagrożenia dla przedsiębiorstwa, dlatego powinny być zarządzane w sposób odmienny niż platformy stacjonarne.

Wyzwania te obejmują zabezpieczenie ich przed różnymi rodzajami ataków, z wykorzystaniem aplikacji i sieci, na urządzenia mobilne, które mają stałe połączenie z Internetem. Urządzenia mobilne mają również potencjalny wpływ na prywatność pracowników korzystających z nich w celach osobistych.

Zarządzanie bezpieczeństwem i prywatnością urządzeń mobilnych w miejscu pracy oraz minimalizowanie związanego z nimi ryzyka może stanowić wyzwanie, ponieważ istnieje wiele różnych narzędzi do zabezpieczania urządzeń mobilnych. Ich prawidłowe wdrożenie może być trudne, ponieważ służące do tego celu metody różnią się znacznie w zależności od narzędzia. Ponadto nieznajomość zagrożeń dla urządzeń mobilnych może zwiększyć wyzwania związane z ich wdrażaniem.

ROZWIĄZANIE

W odpowiedzi na wyzwanie zabezpieczenia urządzeń COPE w przedsiębiorstwie, NIST stworzył przykładowe rozwiązanie w środowisku laboratoryjnym w NCCoE, aby zademonstrować narzędzia zabezpieczające urządzenia mobilne, które przedsiębiorstwa mogą wykorzystać do ochrony swoich sieci. Technologie te są skonfigurowane pod kątem ochrony zasobów organizacji i prywatności użytkowników końcowych, zapewniając metody zwiększania bezpieczeństwa i prywatności wdrażającej je organizacji.

W przykładowym rozwiązaniu wykorzystywane są zarówno urządzenia z systemem Apple iOS, jak i Android. Ponadto obejmuje ono szczegółowe konfiguracje urządzeń i zasady zarządzania mobilnością w przedsiębiorstwie. Podstawą tej architektury są federalne

wytyczne Stanów Zjednoczonych, w tym publikacje z serii NIST 800, Krajowego partnerstwa na rzecz bezpieczeństwa informacji (*ang. National Information Assurance Partnership*), Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (*ang. U.S. Department of Homeland Security*) i Federalnej Rady Głównych Urzędników ds. Informacji (*ang. Federal Chief Information Officers Council*). Te standardy, najlepsze praktyki i programy certyfikacji umożliwiają zapewnienie poufności, integralności i dostępności danych przedsiębiorstwa w systemach mobilnych.

Niniejszy przewodnik zawiera:

- szczegółowe przykładowe rozwiązanie i możliwości dotyczące przeciwdziałania ryzyku i wdrażania środków bezpieczeństwa;
- demonstrację podejścia opartego na produktach dostępnych na rynku;
- instrukcje dla wdrożeniowców i inżynierów bezpieczeństwa, w tym wytyczne dotyczące integracji i konfiguracji przykładowego rozwiązania w ich organizacji przy minimalnym wpływie na procesy operacyjne.

NCCoE poszukiwało istniejących technologii, które zapewniałyby następujące możliwości:

- zwiększoną ochroną danych znajdujących się na urządzeniu mobilnym;
- scentralizowane systemy zarządzania do wdrażania zasad i konfiguracji na urządzeniach;
- ocenę bezpieczeństwa aplikacji mobilnych;
- przeciwdziałanie podsłuchiwaniu danych z urządzeń mobilnych;
- ustawienia prywatności chroniące dane użytkowników końcowych;
- ochronę przed próbami wyłudzenia danych.

Komercyjne, oparte na standardach produkty, takie jak te, z których korzystano, są łatwo dostępne i kompatybilne z istniejącymi technologiami i inwestycjami w infrastrukturę informacyjną (IT).

Chociaż NCCoE wykorzystało pakiet produktów komercyjnych, aby sprostać temu wyzwaniu, niniejszy przewodnik nie promuje tych konkretnych produktów ani nie

gwarantuje zgodności z żadnymi inicjatywami regulacyjnymi. Eksperci ds. bezpieczeństwa informacji w danej organizacji powinni określić, które produkty najlepiej zintegrują się z istniejącymi narzędziami i infrastrukturą systemu IT. Dana organizacja może przyjąć to rozwiązanie lub takie, które jest zgodne z tymi wytycznymi w całości, lub może użyć tego przewodnika jako punktu wyjścia do dostosowania i wdrożenia części rozwiązania.

KORZYŚCI

Przewodnik NCCoE, *Bezpieczeństwo urządzeń mobilnych: Organizacyjne urządzenia mobilne obsługiwane osobiście przez użytkowników (COPE),* może pomóc organizacji:

- zmniejszyć negatywne skutki w przypadku naruszenia bezpieczeństwa urządzenia;
- ograniczyć inwestycje kapitałowe poprzez przyjęcie nowoczesnych modeli mobilności przedsiębiorstwa;
- zastosować niezawodne, oparte na standardach technologie, wykorzystując najlepsze praktyki branżowe;
- ograniczyć ryzyko dla prywatności użytkowników;
- zapewnić lepszą ochronę przed utratą danych osobowych i biznesowych w przypadku kradzieży lub zgubienia urządzenia;
- wdrożyć technologie zarządzania przedsiębiorstwem w celu poprawy bezpieczeństwa należących do niego sieci, urządzeń i aplikacji;
- ograniczyć ryzyko, aby pracownicy mogli uzyskiwać dostęp do niezbędnych danych z niemal dowolnego miejsca, korzystając z szerokiego wyboru urządzeń mobilnych i sieci należących do przedsiębiorstwa;
- poprawić wgląd administratorów systemów w zdarzenia związane z bezpieczeństwem urządzeń mobilnych, zapewniając powiadomienia i identyfikację naruszeń bezpieczeństwa urządzeń i danych;
- wdrożyć rządowe standardy bezpieczeństwa mobilnego.

DZIELENIE SIĘ OPINIAMI

Przewodnik można wyświetlić lub pobrać ze strony https://www.nccoe.nist.gov/projects/building-blocks/mobile- device-security/corporate-owned-personally-enabled.

W przypadku zastosowania tego rozwiązania w swojej organizacji, zachęcamy do podzielenia się z nami doświadczeniami i poradami. Zdajemy sobie sprawę, że same rozwiązania techniczne nie zapewnią pełnych korzyści płynących z naszego rozwiązania, dlatego zachęcamy organizacje do dzielenia się zdobytymi doświadczeniami i najlepszymi praktykami w zakresie przekształcania procesów związanych z wdrażaniem niniejszego przewodnika.

Aby przekazać swoje uwagi lub dowiedzieć się więcej poprzez umówienie się na demonstrację tej przykładowej implementacji, należy skontaktować się z NCCoE, korzystając z adresu mobile-nccoe@nist.gov.

PARTNERZY/WSPÓLNICY W ZAKRESIE TECHNOLOGII

Organizacje uczestniczące w tym projekcie przedstawiły swoje możliwości w odpowiedzi na otwarte zaproszenie w Rejestrze Federalnym USA skierowane do wszystkich źródeł związanych z bezpieczeństwem ze środowisk akademickich i przemysłowych (sprzedawców i integratorów). Następujący respondenci z odpowiednimi możliwościami lub produktami (określeni w niniejszym dokumencie jako „partnerzy/wspólnicy w zakresie technologii") podpisali umowę o współpracy w zakresie badań i rozwoju (*ang. Cooperative Research and Development Agreement – CRADA*) i współdziałali z NIST w ramach konsorcjum w celu stworzenia tego przykładowego rozwiązania.

Tłumaczenie

Niektóre podmioty komercyjne, sprzęt, produkty lub materiały mogą być identyfikowane za pomocą nazwy albo logo firmy lub innych oznaczeń w celu potwierdzenia ich udziału w tej współpracy lub odpowiedniego opisania procedury eksperymentalnej lub koncepcji. Taka identyfikacja nie ma na celu sugerowania specjalnego statusu lub związku z NIST ani rekomendacji lub poparcia przez NIST lub NCCoE. Nie ma też na celu sugerowania, że dane podmioty, sprzęt, produkty lub materiały są bezwzględnie najlepszymi dostępnymi do tego celu.

NIST SP 1800-21B_PL

26 września 2024

Bezpieczeństwo urządzeń mobilnych: Organizacyjne urządzenia mobilne obsługiwane osobiście przez użytkowników (COPE)

Tom B
Podejście, architektura i charakterystyka bezpieczeństwa

NIST SPECIAL PUBLICATION 1800-B

Mobile Device Security:
Corporate-Owned Personally-Enabled (COPE)

Volume B:
Approach, Architecture, and Security Characteristics

Joshua M. Franklin*
Gema Howell
Kaitlin Boeckl
Naomi Lefkovitz
Ellen Nadeau*
Applied Cybersecurity Division
Information Technology Laboratory

Dr. Behnam Shariati
University of Maryland, Baltimore County
Department of Computer Science and Electrical Engineering
Baltimore, Maryland

Jason G. Ajmo
Christopher J. Brown
Spike E. Dog
Frank Javar
Michael Peck
Kenneth F. Sandlin
The MITRE Corporation
McLean, Virginia

Former employee; all work for this publication done while at employer

September 2020

Final

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-21

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

National Cybersecurity Center of Excellence (NCCoE), będąca częścią Narodowego Instytutu Standaryzacji i Technologii (*ang. National Institute of Standards and Technology – NIST*), jest ośrodkiem współpracy, w którym organizacje branżowe, agencje rządowe i instytucje akademickie współdziałają w celu rozwiązania najbardziej palących kwestii związanych z cyberbezpieczeństwem dla przedsiębiorstw. Taka współpraca pomiędzy sektorem publicznym i prywatnym umożliwia tworzenie praktycznych rozwiązań w zakresie cyberbezpieczeństwa dla konkretnych branż, a także dla dużych, międzysektorowych wyzwań technologicznych. Poprzez konsorcja działające w ramach umów o współpracy w zakresie badań i rozwoju (*ang. Cooperative Research and Development Agreements – CRADA*), w tym partnerów technologicznych – od liderów rynku Fortune 50 po mniejsze firmy specjalizujące się w bezpieczeństwie technologii informatycznych – NCCoE stosuje standardy i najlepsze praktyki w celu opracowania modułowych, elastycznych przykładowych rozwiązań z zakresu cyberbezpieczeństwa przy użyciu komercyjnie dostępnych technologii. NCCoE dokumentuje te przykładowe rozwiązania w serii publikacji NIST 1800, w której zestawiono możliwości z Ramami cyberbezpieczeństwa NIST i wyszczególniono kroki potrzebne innemu podmiotowi do odtworzenia przykładowego rozwiązania. NCCoE zostało utworzone w 2012 r. przez NIST we współpracy ze stanem Maryland i hrabstwem Montgomery w stanie Maryland.

Więcej informacji na temat NCCoE można znaleźć na stronie https://www.nccoe.nist.gov.

Więcej informacji na temat NIST można znaleźć na stronie https://www.nist.gov.

PRZEWODNIKI NIST DOTYCZĄCE PRAKTYK W ZAKRESIE CYBERBEZPIECZEŃSTWA

Przewodniki NIST dotyczące praktyk w zakresie cyberbezpieczeństwa (seria publikacji specjalnych 1800) dotyczą konkretnych wyzwań związanych z cyberbezpieczeństwem w sektorze publicznym i prywatnym. Są to praktyczne, przyjazne dla użytkownika

przewodniki, które ułatwiają przyjęcie opartego na standardach podejścia do cyberbezpieczeństwa. Służą one do demonstrowania członkom społeczności zajmującej się bezpieczeństwem informacji, jak wdrażać przykładowe rozwiązania, które umożliwiają im dostosowanie się do odpowiednich standardów i najlepszych praktyk, a także dostarczają użytkownikom listy materiałów, pliki konfiguracyjne i inne informacje potrzebne do wdrożenia podobnego podejścia.

W dokumentach z tej serii opisano przykładowe wdrożenia praktyk z zakresu cyberbezpieczeństwa, które firmy i inne organizacje mogą dobrowolnie przyjąć. Nie są to przepisy ani obowiązkowe praktyki, nie mają one również mocy prawnej.

STRESZCZENIE

Urządzenia mobilne zapewniają dostęp do istotnych zasobów w miejscu pracy, jednocześnie zapewniając pracownikom elastyczność przy wykonywaniu codziennych czynności. Zabezpieczenie tych urządzeń ma kluczowe znaczenie dla ciągłości operacji biznesowych.

Urządzenia mobilne mogą zwiększyć wydajność i produktywność, ale mogą również stanowić źródło zagrożenia dla wrażliwych danych. Narzędzia do zarządzania urządzeniami mobilnymi mogą przeciwdziałać takim zagrożeniom, umożliwiając zabezpieczenie dostępu do sieci i zasobów. Narzędzia te różnią się od tych wykorzystywanych do zabezpieczenia typowej komputerowej stacji roboczej.

Ten praktyczny przewodnik koncentruje się na ulepszeniach zabezpieczeń, które można wprowadzić na firmowych urządzeniach mobilnych do użytku osobistego (COPE). Urządzenia COPE są własnością przedsiębiorstwa i są przydzielane pracownikom. Zarówno przedsiębiorstwo, jak i pracownik mogą instalować aplikacje na urządzeniu.

Aby sprostać wyzwaniu zabezpieczenia urządzeń mobilnych COPE przy jednoczesnym zarządzaniu ryzykiem, NCCoE w ramach NIST stworzyło architekturę referencyjną,

aby pokazać, w jaki sposób różne technologie bezpieczeństwa mobilnego[3] mogą być zintegrowane z siecią przedsiębiorstwa.

W niniejszym przewodniku po praktykach w zakresie cyberbezpieczeństwa NIST opisano, w jaki sposób organizacje mogą korzystać ze standardowych produktów dostępnych na rynku, aby zaspokoić swoje potrzeby w zakresie bezpieczeństwa i prywatności urządzeń mobilnych.

SŁOWA KLUCZOWE

Własność firmy dostępna prywatnie (*ang. Corporate-owned personally-enabled– COPE*); zarządzanie urządzeniami mobilnymi (*ang. mobile device management*); bezpieczeństwo urządzeń mobilnych (*ang. mobile device security*), lokalne (*ang.* on *premise)*; *przynieś własne urządzenie* (*ang. bring your own device – BYOD)*

[3] Także: technologie zabezpieczeń mobilnych

Partnerzy/wspólnicy w zakresie technologii, którzy uczestniczyli w tym projekcie, przedstawili swoje możliwości w odpowiedzi na ogłoszenie w Rejestrze Federalnym USA. Respondenci dysponujący odpowiednimi możliwościami lub produktami zostali zaproszeni do podpisania z NIST umowy o współpracy w zakresie badań i rozwoju (*ang. Cooperative Research and Development Agreement – CRADA*), umożliwiającej im udział w konsorcjum w celu zbudowania tego przykładowego rozwiązania. Współpracowaliśmy z:

Partner/wspólnik w zakresie technologii	**Zakres udziału**
Appthority*	Appthority Cloud Service, Mobile Threat Intelligence
Kryptowire	Kryptowire Cloud Service, Application Vetting
Lookout	Lookout Cloud Service/Lookout Agent w wersji 5.10.0.142 (iOS), 5.9.0.420 (Android), Mobile Threat Defense
MobileIron	MobileIron Core w wersji 9.7.0.1, MobileIron Agent w wersji 11.0.1A (iOS), 10.2.1.1.3R (Android), Enterprise Mobility Management
Palo Alto Networks	Palo Alto Networks PA-220
Qualcomm	Qualcomm Trusted Execution Environment (wersja zależy od urządzenia)

* Appthority (firma przejęta przez Symantec – oddział Broadcom).

1. PODSUMOWANIE

W niniejszym punkcie czytelnik zapozna się z następującymi zagadnieniami:

- koncepcje urządzeń będących własnością firmy wykorzystywanych przez pracowników również do celów prywatnych (*ang. Corporate-Owned Personally-Enabled – COPE*);
- wyzwania, rozwiązania i korzyści z COPE związane z niniejszym przewodnikiem po praktykach.

Urządzenia mobilne COPE są własnością przedsiębiorstwa i są przydzielane pracownikom. Zarówno przedsiębiorstwo, jak i pracownik mogą instalować aplikacje na urządzeniu.

Niniejszy przewodnik po praktykach cyberbezpieczeństwa Narodowego Instytutu Standardów i Technologii (*ang. National Institute of Standards and Technology – NIST*) ma na celu ułatwienie sprostania wyzwaniom związanym z wdrażaniem zabezpieczeń urządzeń mobilnych COPE na kilka sposobów: analizując zestaw zagrożeń dla bezpieczeństwa i prywatności urządzeń mobilnych, analizując technologie zabezpieczające oraz przedstawiając projekt referencyjny oparty na tych technologiach, umożliwiający przeciwdziałanie zidentyfikowanym zagrożeniom.

Urządzenia mobilne zapewniają większą elastyczność uzyskiwania dostępu do zasobów przez pracowników. W przypadku niektórych organizacji elastyczność ta umożliwia zastosowanie podejścia hybrydowego, łączącego procesy realizowane w biurze z komunikacją i przepływami pracy na urządzeniach mobilnych.

W przypadku innych firm elastyczność ta, w połączeniu z rosnącą funkcjonalnością urządzeń mobilnych, umożliwia przyjęcie podejścia *mobile-first*, w którym pracownicy komunikują się i współpracują głównie za pomocą urządzeń mobilnych. Jednak pewne funkcje, które czynią urządzenia mobilne coraz bardziej elastycznymi i funkcjonalnymi, sprawiają również, że ich wdrażanie i zarządzanie nimi z myślą o bezpieczeństwie staje się wyzwaniem.

Jednocześnie organizacje stają się coraz bardziej świadome konsekwencji dla prywatności, które wynikają z korzystania z technologii bezpieczeństwa urządzeń

mobilnych. Dlatego opracowanie skutecznej strategii wdrożenia urządzeń mobilnych wymaga od organizacji oceny jej wymagań w zakresie bezpieczeństwa i prywatności.

Aby pomóc organizacjom w radzeniu sobie z zagrożeniami związanymi z bezpieczeństwem i prywatnością urządzeń mobilnych, projekt referencyjny zawarty w niniejszym dokumencie obejmuje:

- opis przykładowego rozwiązania do wdrażania urządzeń mobilnych, obejmującego lokalne rozwiązanie do zarządzania mobilnością w przedsiębiorstwie (*ang.* on-premises *Enterprise Mobility Management – EMM*) zintegrowane z technologiami bezpieczeństwa mobilnego opartymi na chmurze i agentach, aby ułatwić wdrożenie zestawu funkcji bezpieczeństwa i prywatności wspomagających realizację scenariusza wykorzystania urządzeń mobilnych COPE;
- serię instrukcji krok po kroku obejmujących wstępne procesy (instalację lub udostępnianie) i konfigurację dla każdego elementu architektury, aby ułatwić inżynierom ds. bezpieczeństwa szybkie wdrożenie i ocenę naszego przykładowego rozwiązania w ich środowisku testowym.

W przykładowym rozwiązaniu przedmiotowego projektu referencyjnego wykorzystano dostępne na rynku standardowe produkty. Może ono być wykorzystane bezpośrednio przez dowolną organizację realizującą scenariusz COPE poprzez wdrożenie infrastruktury bezpieczeństwa, która umożliwi integrację lokalnych i hostowanych w chmurze mobilnych technologii bezpieczeństwa.

Organizacja może również wykorzystać projekt referencyjny i przykładowe rozwiązanie w całości lub w części jako podstawę do stworzenia rozwiązania niestandardowego, zapewniającego właściwości w zakresie bezpieczeństwa i prywatności, które najlepiej wspomagają realizację jej unikalnego scenariusza użytkowania urządzeń mobilnych.

1.1. WYZWANIE

Urządzenia mobilne są nieodłącznym elementem nowoczesnych miejsc pracy, a ponieważ pracownicy używają ich do wykonywania zadań, przed organizacjami stoi wyzwanie

polegające na zapewnieniu, że urządzenia te przetwarzają, modyfikują i przechowują wrażliwe dane w bezpieczny sposób. Niosą one ze sobą unikalne zagrożenia dla przedsiębiorstwa i muszą być zarządzane inaczej niż platformy stacjonarne.

Ze względu na ich unikalne możliwości, specyficzne wymagania dotyczące bezpieczeństwa urządzeń mobilnych mogą obejmować:

- zabezpieczenie ich stale aktywnych połączeń z Internetem przed atakami sieciowymi;
- zabezpieczanie danych na urządzeniach, aby zapobiec naruszeniu ich bezpieczeństwa przez złośliwe aplikacje;
- ochronę przed próbami wyłudzenia danych uwierzytelniających użytkownika lub nakłonienia go do zainstalowania oprogramowania;
- wybieranie spośród wielu dostępnych narzędzi do zarządzania urządzeniami mobilnymi i konsekwentne wdrażanie ich funkcji ochrony;
- identyfikowanie zagrożeń dla urządzeń mobilnych i sposobów przeciwdziałania im.

Ze względu na te wyzwania, zarządzanie bezpieczeństwem pracy urządzeń mobilnych i minimalizowanie stwarzanego przez nie ryzyka może być skomplikowane. Zapewniając przykładowe rozwiązanie, z którego organizacje mogą natychmiast skorzystać, niniejszy przewodnik upraszcza wdrażanie funkcji bezpieczeństwa urządzeń mobilnych.

1.2. ROZWIĄZANIE

W laboratorium National Cybersecurity Center of Excellence (NCCoE) inżynierowie NIST zbudowali środowisko, które zawiera przykładowe rozwiązanie do zarządzania bezpieczeństwem urządzeń mobilnych. W przewodniku pokazano, w jaki sposób przedsiębiorstwo może wykorzystać tę infrastrukturę do wdrożenia lokalnego systemu EMM, a także systemów ochrony przed zagrożeniami dla urządzeń mobilnych (*ang. Mobile Threat Defense – MTD*), analizy zagrożeń dla urządzeń mobilnych (*ang. Mobile Threat Intelligence – MTI*), weryfikacji aplikacji, bezpiecznego uwierzytelniania rozruchu/obrazu i usług wirtualnej sieci prywatnej (*ang. Virtual Private Network – VPN*).

Co więcej, technologie te zostały skonfigurowane pod kątem ochrony zasobów organizacji i prywatności użytkowników końcowych, zapewniając metodologie zwiększające poziom bezpieczeństwa wdrażającej je organizacji. Podstawą tej architektury są federalne wytyczne Stanów Zjednoczonych, w tym publikacje z serii NIST 800 [1], inicjatywa Krajowego partnerstwo na rzecz bezpieczeństwa informacji (*ang. National Information Assurance Partnership - NIAP*) [2], Departament Bezpieczeństwa Wewnętrznego [3] oraz Federalna Rada Głównych Urzędników ds. Informacji (*ang. Chief Information Officer – CIO*) [4]. Te standardy, najlepsze praktyki i programy certyfikacji umożliwiają zapewnienie poufności, integralności i dostępności danych przedsiębiorstwa w systemach mobilnych.

Niniejszy przewodnik zawiera:

- szczegółowe przykładowe rozwiązanie z funkcjami umożliwiającymi przeciwdziałanie powszechnym zagrożeniom dla urządzeń mobilnych;
- demonstrację podejścia opartego na produktach dostępnych na rynku;
- instrukcje instalacji krok po kroku dla wdrożeniowców, które mają na celu integrację z istniejącymi systemami w celu poprawy stanu bezpieczeństwa urządzeń mobilnych organizacji przy minimalnym zakłóceniu jej działalności.

NCCoE poszukiwało istniejących technologii, które zapewniałyby następujące możliwości:

- ochronę danych przetwarzanych w urządzeniach mobilnych;
- wykorzystywanie scentralizowanych systemów zarządzania do wdrażania zasad i konfiguracji na urządzeniach;
- weryfikację bezpieczeństwa aplikacji mobilnych;
- ochronę danych przed podsłuchem;
- konfigurację ustawień prywatności w celu zapewnienia przewidywalności, zarządzania i odłączanie (anonimizację) informacji umożliwiających identyfikację użytkownika końcowego (*ang. Personal Identifiable Information – PII*) użytkowników końcowych.

Komercyjne, oparte na standardach produkty, takie jak te, z których korzystano w środowisku testowym, są łatwo dostępne i kompatybilne z istniejącymi technologiami i inwestycjami w infrastrukturę (IT).

1.2.1. NORMY I WYTYCZNE

W niniejszym przewodniku wykorzystano wiele norm i wytycznych, w tym dokumenty: NIST *Cybersecurity Framework Version 1* [5], NIST *Privacy Risk Assessment Methodology (PRAM)* [6], *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [7], NIST *Risk Management Framework* [8], oraz *NIST Mobile Threat Catalogue* [9]. Dodatkowe informacje można znaleźć w załączniku D, „Normy i wytyczne".

1.3. KORZYŚCI

Potencjalne korzyści płynące z przykładowego rozwiązania badanego w ramach tego projektu są następujące:

- zapewnienie użytkownikom lepszej ochrony zarówno przed złośliwymi aplikacjami, jak i utratą danych osobowych i biznesowych w przypadku kradzieży lub zgubienia urządzenia;
- ograniczenie negatywnych skutków dla organizacji w przypadku naruszenia bezpieczeństwa urządzenia;
- ograniczenie inwestycji kapitałowych poprzez przyjęcie nowoczesnych modeli mobilności przedsiębiorstwa;
- zapewnienie administratorom systemu wglądu w zdarzenia związane z bezpieczeństwem urządzeń mobilnych, umożliwiając automatyczną identyfikację i powiadamianie o naruszeniu bezpieczeństwa urządzenia;
- zapewnienie modułowej architektury opartej na rolach związanych z technologią, przy jednoczesnym zachowaniu niezależności od dostawcy;
- ułatwianie stosowania wielu scenariuszy korzystania z urządzeń mobilnych przy użyciu urządzeń COPE;

- stosowanie niezawodnych technologii opartych na standardach wykorzystujących najlepsze praktyki branżowe;
- przedstawienie sposobów bezpiecznego mobilnego dostępu do zasobów organizacji;
- zilustrowanie zastosowania ram zarządzania ryzykiem NIST do scenariuszy związanych z urządzeniami mobilnymi.

2. SPOSÓB KORZYSTANIA Z NINIEJSZEGO PRZEWODNIKA

W niniejszym punkcie czytelnik zapozna się z następującymi zagadnieniami:

- zawartość niniejszego przewodnika po praktykach;
- sugerowani odbiorcy każdego z tomów;
- konwencje typograficzne stosowane w niniejszym tomie.

W niniejszym przewodniku po praktykach w zakresie cyberbezpieczeństwa NIST przedstawiono projekt referencyjny oparty na standardach i zapewniający użytkownikom informacje potrzebne do odtworzenia sposobu poprawy bezpieczeństwa i prywatności urządzeń mobilnych należących do organizacji. Przedmiotowy projekt referencyjny jest modułowy i może być wdrażany w całości lub w części.

Niniejszy przewodnik obejmuje trzy tomy:

- NIST SP 1800-21A: *Streszczenie*.
- NIST SP 1800-21B: *Podejście, architektura i charakterystyka bezpieczeństwa* – co zbudowaliśmy i dlaczego **(jesteś tutaj)**.
- NIST SP 1800-21C: *Poradniki „How-to”* – instrukcje dotyczące tworzenia przykładowego rozwiązania.

  W zależności od roli pełnionej w organizacji, z niniejszego przewodnika można korzystać na różne sposoby:

Osoby podejmujące decyzje biznesowe, w tym osoby kluczowe ds. bezpieczeństwa i technologii będą zainteresowani streszczeniem, NIST SP 1800-21A, w którym poruszono następujące tematy:

- wyzwania stojące przed przedsiębiorstwami w zakresie zabezpieczania przed zagrożeniami urządzeń mobilnych należących do organizacji, które to wyzwania są inne niż w przypadku platform stacjonarnych;
- przykładowe rozwiązanie zbudowane w NCCoE;
- korzyści z wdrożenia przykładowego rozwiązania.

Menedżerowie ds. technologii lub programów bezpieczeństwa, którzy są zainteresowani tym, jak identyfikować, rozumieć, oceniać i ograniczać ryzyko, będą zainteresowani tą częścią przewodnika, *NIST SP 1800-21B*, w której opisano, co zrobiono i dlaczego. Szczególnie pomocne będą dla nich poniższe punkty:

- Punkt 3.4, „Ocena ryzyka", który zawiera opis przeprowadzonej analizy ryzyka;
- Punkt 4.3, „Mapa środków bezpieczeństwa", zawierający porównanie charakterystyki bezpieczeństwa tego przykładowego rozwiązania ze standardami cyberbezpieczeństwa i najlepszymi praktykami.

Streszczenie, *NIST SP 1800-21A*, można udostępnić członkom zespołu kierowniczego, aby pomóc im zrozumieć znaczenie wdrożenia rozwiązań opartych na standardach w celu poprawy bezpieczeństwa urządzeń mobilnych za pomocą lokalnych rozwiązań do zarządzania urządzeniami mobilnymi.

Specjaliści IT, którzy chcą wdrożyć takie podejście, uznają cały przewodnik za przydatny. Mogą skorzystać z części zawierającej poradnik, *NIST SP 1800-21C*, aby odtworzyć całość lub część rozwiązania stworzonego w laboratorium NCCoE. Część dokumentu zawierająca poradnik obejmuje szczegółowe instrukcje dotyczące instalacji, konfiguracji i integracji produktów w celu wdrożenia przykładowego rozwiązania. Nie powielamy dokumentacji od twórców produktów, która jest powszechnie dostępna. Pokazujemy raczej, w jaki sposób włączyliśmy produkty do naszego środowiska, aby stworzyć przykładowe rozwiązanie.

W niniejszym przewodniku założono, że specjaliści ds. technologii informacyjnych (IT) mają doświadczenie we wdrażaniu produktów zabezpieczających w przedsiębiorstwie. W celu sprostania wyzwaniu wykorzystaliśmy szereg produktów komercyjnych, jednak niniejszy przewodnik nie ma na celu promowania tych konkretnych produktów. Dana organizacja może przyjąć to rozwiązanie lub takie, które jest zgodne z tymi wytycznymi w całości, lub można użyć tego przewodnika jako punktu wyjścia do dostosowania i wdrożenia części przykładowego rozwiązania z tego przewodnika do lokalnego zarządzania bezpieczeństwem urządzeń mobilnych. Eksperci ds. bezpieczeństwa w danej organizacji powinni określić, które produkty najlepiej

zintegrują się z istniejącymi narzędziami i infrastrukturą systemu IT. Mamy nadzieję, że użytkownicy będą poszukiwać produktów zgodnych z obowiązującymi standardami i najlepszymi praktykami. Punkt 3.6, „Technologie", zawiera listę produktów, z których korzystaliśmy, a w załączniku I powiązano je ze środkami cyberbezpieczeństwa stosowanymi w ramach opisywanego rozwiązania referencyjnego.

W przewodniku NIST po praktykach w zakresie cyberbezpieczeństwa nie opisano ostatecznego rozwiązania problemu, ale możliwe rozwiązanie.

Komentarze, sugestie i historie pomyślnego wdrożenia umożliwią ulepszenie kolejnych wersji niniejszego przewodnika. Prosimy o przesłanie swoich opinii na adres mobile-nccoe@nist.gov.

2.1. KONWENCJE TYPOGRAFICZNE

W poniższej tabeli przedstawiono konwencje typograficzne stosowane w niniejszym tomie.

Krój pisma/symbol	Znaczenie	Przykład
Kursywa	nazwy plików i nazwy ścieżek; odniesienia do dokumentów, które nie są hiperłączami; nowe terminy; i symbole zastępcze	Szczegółowe definicje terminów można znaleźć w Glosariuszu NCCoE.
Pogrubienie	nazwy menu, opcji, przycisków poleceń i pól	Choose **File (Wybierz plik) > Edit (Edytuj)**.
Czcionka o stałej szerokości znaków	dane wejściowe wiersza poleceń, dane wyjściowe komputera na ekranie, przykładowy kod i kody stanu	mkdir
Pogrubiona czcionka o stałej szerokości znaków	dane wprowadzane przez użytkownika w wierszu poleceń zestawione z danymi wyjściowymi komputera	**service sshd start**
niebieski tekst	łącze do innej części dokumentu, adres URL strony internetowej lub adres e-mail	Wszystkie publikacje NCCoE (NIST) są dostępne pod adresem https://www.nccoe.nist.gov.

3. PODEJŚCIE

W niniejszym punkcie czytelnik zapozna się z następującymi zagadnieniami:

- docelowi odbiorcy, zakres i założenia niniejszego przewodnika;
- fikcyjna organizacja wykorzystana w przykładowym scenariuszu;
- szacowanie ryzyka, w tym szacowanie ryzyka dla prywatności;
- cele przykładowego rozwiązania i wykorzystywane technologie.

Zespół projektowy NIST przeanalizował raporty dotyczące trendów w zakresie bezpieczeństwa urządzeń mobilnych i wystosował otwarte zaproszenie do społeczności zajmującej się tym zagadnieniem — w tym dostawców, naukowców, administratorów i użytkowników — do udziału w dyskusji na temat pilnych wyzwań związanych z cyberbezpieczeństwem. Społeczność ta dostarczyła dwóch istotnych informacji.

Po pierwsze, administratorzy są zdezorientowani co do tego, które zasady i standardy z niezliczonych źródeł należy wdrażać. Po drugie, użytkownicy urządzeń mobilnych są niezadowoleni ze stopnia, w jakim organizacje kontrolują ich urządzenia mobilne i utrzymują wgląd w ich osobistą aktywność.

W związku z tym zespół NIST dokonał przeglądu podstawowych standardów, najlepszych praktyk i wytycznych ze źródeł rządowych i wdrożył scenariusz COPE w swoim projekcie. W ramach tego przedsięwzięcia zwrócono uwagę na kilka cech i możliwości związanych z bezpieczeństwem, które zostały udokumentowane w ramach modułu *Mobile Device Security for Enterprises* [10].

3.1. ODBIORCY

Niniejszy przewodnik po praktykach jest przeznaczony dla organizacji, które chcą zwiększyć poziom bezpieczeństwa i prywatności firmowych urządzeń mobilnych. Jest on przeznaczony dla kadry kierowniczej, menedżerów ds. bezpieczeństwa, inżynierów, administratorów i innych osób odpowiedzialnych za pozyskiwanie, wdrażanie i utrzymywanie firmowych technologii mobilnych, w tym scentralizowanego systemu zarządzania urządzeniami, weryfikacji aplikacji i ochrony punktów końcowych.

Dokument ten będzie szczególnie interesujący dla architektów systemów już zarządzających rozwiązaniami mobilnymi i tych, którzy chcą wdrożyć urządzenia mobilne w najbliższym czasie. Zakłada się w nim, że czytelnicy mają podstawową wiedzę na temat technologii urządzeń mobilnych i zasad bezpieczeństwa przedsiębiorstw. Informacje na temat tego, jak różni odbiorcy mogą efektywnie korzystać z niniejszego przewodnika, znajdują się w rozdziale 2.

3.2. ZAKRES

Zakres niniejszego produktu obejmuje zarządzanie telefonami komórkowymi i tabletami za pomocą lokalnego systemu EMM. Urządzenia mobilne są powszechnie definiowane jako:

Przenośne urządzenia komputerowe, które: (I) mieszczą się w niewielkiej obudowie, dzięki czemu mogą być łatwo przenoszone przez jedną osobę; (II) są zaprojektowane do działania bez fizycznego połączenia (np. bezprzewodowego przesyłania lub odbierania informacji); (III) są wyposażone w lokalną, niewymienną lub wymienną pamięć masową; oraz (IV) mają niezależne źródło zasilania. Urządzenia mobilne mogą również być wyposażone w funkcje komunikacji głosowej, wbudowane czujniki umożliwiające przechwytywanie informacji i/lub wbudowane funkcje synchronizacji danych lokalnych z lokalizacjami zdalnymi. Przykłady: smartfony, tablety i e-czytniki [11].

Laptopy zostały wyłączone z zakresu niniejszej publikacji, ponieważ dostępne obecnie środki bezpieczeństwa dla laptopów znacznie różnią się od tych przeznaczonych dla telefonów komórkowych i tabletów, choć zmienia się to wraz z pojawieniem się ujednoliconych narzędzi do zarządzania punktami końcowymi.

Urządzenia o minimalnych możliwościach obliczeniowych również nie są brane pod uwagę, w tym starsze modele telefonów, urządzenia wbudowane w ubrania i urządzenia klasyfikowane jako część Internetu rzeczy (*ang. Internet of Things. – IoT*). Niniejsza publikacja nie obejmuje niejawnych systemów, urządzeń, danych i aplikacji.

Zespół projektowy opracował fikcyjny scenariusz oparty na wymyślonej organizacji (Orvilia Development), aby zapewnić kontekst dla naszego szacowania ryzyka

i umożliwić nam stworzenie projektu referencyjnego w celu rozwiązania typowych wyzwań związanych z bezpieczeństwem urządzeń mobilnych w organizacjach. Wykorzystanie fikcyjnego scenariusza umożliwia zilustrowanie problemów, z jakimi organizacja może się zetknąć podczas rozwiązywania typowych wyzwań związanych z bezpieczeństwem urządzeń mobilnych w przedsiębiorstwie. Dążyliśmy do tego, aby przykładowe rozwiązanie zaproponowane w niniejszym przewodniku po praktykach miało zastosowanie do szerokiego grona przedsiębiorstw, w tym zarówno z sektora publicznego, jak i prywatnego.

Przykładowe rozwiązanie nie uwzględnia zagrożeń wewnętrznych i związanych z nimi środków zaradczych. Koncentruje się na zagrożeniach zewnętrznych i na tym, jak przykładowe rozwiązanie może im przeciwdziałać.

Dodatkowe opcje wdrażania urządzeń z systemami Android, Apple i Samsung Knox zostały omówione w załączniku E.

3.2.1. ORVILIA DEVELOPMENT

Fikcyjna organizacja, Orvilia Development, jest start-upem świadczącym usługi IT wielu organizacjom z sektora prywatnego. Jej oferta usług obejmuje tworzenie skalowalnych aplikacji internetowych, ulepszanie istniejących systemów IT, zarządzanie projektami i zaopatrzenie. Orvilia niedawno wygrała swój pierwszy kontrakt rządowy. Biorąc pod uwagę obecny poziom bezpieczeństwa w organizacji, zwłaszcza w zakresie korzystania z urządzeń mobilnych, zapewnienie zgodności z przepisami rządowymi i zaostrzonymi standardami cyberbezpieczeństwa stawia przed nią nowe wyzwania.

Orvilia wdrożyła lokalne zasoby IT. Hostuje własną domenę Microsoft Active Directory (AD), serwer poczty elektronicznej Microsoft Exchange oraz zasoby internetowe dla pracowników, takie jak rejestracja czasu pracy i obsługa podróży/wyjść. Pracownicy mogą uzyskiwać bezpośredni dostęp do wszystkich zasobów przedsiębiorstwa lokalnie lub zdalnie z dowolnego urządzenia podłączonego do Internetu z wykorzystaniem uwierzytelniania opartego na hasłach.

Orvilia zapewnia również swoim pracownikom firmowe urządzenia mobilne. Mogą one być wykorzystywane do działań prywatnych, w tym połączeń telefonicznych, obsługi komunikatorów internetowych oraz instalowania aplikacji społecznościowych i korzystania z nich. Pracownicy regularnie wykonują również swoje obowiązki poza biurem i często korzystają z publicznych sieci Wi-Fi w hotelach, na lotniskach i w kawiarniach.

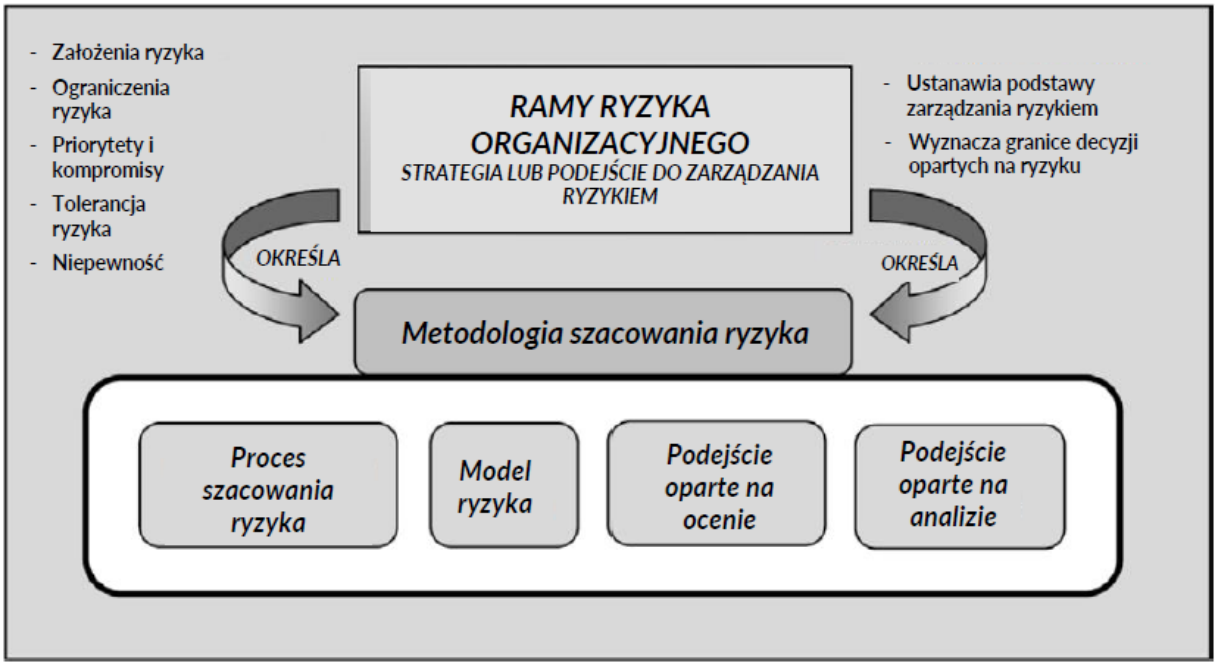
Praktyka wdrażania urządzeń mobilnych w firmie Orvilia wciąż jest na etapie rozwoju. Organizacja wprowadziła minimalne zasady dotyczące urządzeń mobilnych i nie wdrożyła żadnych dodatkowych mechanizmów bezpieczeństwa, takich jak system zarządzania urządzeniami mobilnymi w przedsiębiorstwie. Wszystkie działania związane z zasadami i egzekwowaniem wymogów bezpieczeństwa są wykonywane ręcznie i doraźnie. Oczekuje się, że pracownicy będą zabezpieczać własne urządzenia COPE, na przykład poprzez regularne instalowanie aktualizacji systemu operacyjnego (*ang. Operating System – OS*), oraz będą kierować się zdrowym rozsądkiem przy korzystaniu z nich do celów osobistych.

Nie wprowadzono jednak żadnych mechanizmów zapobiegających przypadkom niewłaściwego użycia lub naruszenia bezpieczeństwa urządzeń lub wykrywających je. Co więcej, polityka organizacji zabrania dostępu do sieci firmowej z osobistych urządzeń mobilnych, ale nie wdrożono żadnych technicznych zabezpieczeń, aby uniemożliwić pracownikom takie działania. Taki stan bezpieczeństwa wynikał z niewielkich rozmiarów organizacji, wysokiego poziomu wiedzy technicznej pracowników i braku wiedzy o jakichkolwiek incydentach z zakresu cyberbezpieczeństwa, które miałyby na nią znaczący wpływ.

Jednak nowy status Orvilii jako kontrahenta cywilnej agencji rządowej wymaga od niej osiągnięcia i utrzymania zgodności z polityką rządową, która wymaga przestrzegania najlepszych praktyk w zakresie cyberbezpieczeństwa i obowiązujących standardów. Na przykład Orvilia jest zobowiązana do zabezpieczenia dostępu i przechowywania wrażliwych informacji rządowych, do których jej pracownicy będą musieli uzyskiwać dostęp ze swoich urządzeń mobilnych – zarówno lokalnie w siedzibach agencji, jak i zdalnie z biura organizacji lub podczas podróży.

Oprócz konieczności spełnienia wymogów zgodności wynikających ze zobowiązań zawartych w umowie z agencją rządową, kierownictwo Orvilia obawia się również o potencjalne przyszłe incydenty, w których atakujący z innych państw mogliby uzyskać wrażliwe dane rządowe z niezabezpieczonych urządzeń i infrastruktury.

W związku z tym przeprowadzono szacowanie ryzyka zgodnie z opisem w publikacji NIST SP 800-30[4] w wersji 1, *Guide for Conducting Risk Assessments* [12], wykorzystując koncepcje zarządzania ryzykiem przedstawione na rysunku 3-1.



Rysunek 3-1 Podejście do zarządzania ryzykiem

Szacowanie ryzyka wykazało, że obecna infrastruktura mobilna Orvilii naraża organizację na ryzyko włamania i naruszenia wrażliwych danych. Wyniki procesu szacowania ryzyka przedstawiono w załączniku F.

Na podstawie wyników szacowania ryzyka organizacja Orvilia zdecydowała się zainwestować w poprawę bezpieczeństwa swojej infrastruktury mobilnej. Szczegółowe informacje na temat nowej infrastruktury bezpieczeństwa urządzeń mobilnych organizacji Orvilia znajdują się w rozdziale 4. Jak opisano w projekcie

[4] Polskojęzyczny dokument NSC 800-30.

architektury w rozdziale 4, nowa infrastruktura organizacji Orvilia odpowiada na zagrożenia zidentyfikowane w ramach szacowania ryzyka. Zespół ds. szacowania ryzyka dokonał przeglądu wytycznych organizacji normalizacyjnych i agencji rządowych, a następnie określił standardy i wytyczne mające zastosowanie do przypadku użycia urządzeń mobilnych w organizacji, które zostały określone w załączniku D.

3.3. ZAŁOŻENIA

Projekt ten opiera się na następujących założeniach:

- Rozwiązanie zostało opracowane w środowisku laboratoryjnym opartym na typowej infrastrukturze IT przedsiębiorstwa. Nie odzwierciedla on złożoności środowiska produkcyjnego.
- Organizacja ma dostęp do umiejętności i zasobów wymaganych do wdrożenia rozwiązania zabezpieczającego urządzenia mobilne.
- Korzyści płynące z przyjęcia tego konkretnego rozwiązania zabezpieczającego urządzenia mobilne przeważają nad wszelkimi dodatkowymi zagrożeniami dla wydajności, niezawodności lub bezpieczeństwa, które mogą w związku z nim wystąpić. Pragniemy jednak zwrócić uwagę czytelnika na fakt, że wdrożenie jakichkolwiek środków bezpieczeństwa może potencjalnie zwiększyć lub zmniejszyć obszar podatny na atak w przedsiębiorstwie, przy czym ich rzeczywiste skutki będą się różnić w zależności od organizacji. Ponieważ środowisko organizacyjne, w którym niniejszy projekt mógłby zostać wdrożony, charakteryzuje się większym poziomem złożoności, niż zostało to ujęte w niniejszym przewodniku, zakładamy, że organizacje najpierw przeanalizują implikacje dla ich obecnego środowiska przed wdrożeniem jakiejkolwiek części proponowanego rozwiązania.
- Organizacje albo już zainwestowały, albo są skłonne zainwestować w bezpieczeństwo urządzeń mobilnych używanych w ich organizacji i w ich systemach IT. w związku z tym zakładamy, że albo mają technologię, która będzie obsługiwać wdrożenie, albo mają dostęp do gotowej technologii bezpieczeństwa

informacji zastosowanej w tym projekcie, która, jak zakładamy, będzie działać zgodnie z opisem odpowiedniego dostawcy produktu.

- Organizacje zapoznały się z istniejącymi standardami i wszelkimi powiązanymi wytycznymi (np. ramami cyberbezpieczeństwa NIST [5], NIST SP 800-124 w wersji 2 projektu [13], NIST SP 1800-4 [14]) istotnymi dla wdrożenia rozwiązania zaproponowanego w niniejszym przewodniku. Zakładamy również, że wszelkie istniejące technologie, które mają być wykorzystane w proponowanym rozwiązaniu, zostały wdrożone w sposób zgodny z tymi standardami.
- Organizacje wprowadziły odpowiednie zasady bezpieczeństwa urządzeń mobilnych, które zostaną zaktualizowane w oparciu o wdrożenie tego rozwiązania.

3.3.1. INŻYNIERIA SYSTEMÓW

Niektóre organizacje stosują podejście oparte na inżynierii systemów w planowaniu i wdrażaniu swoich projektów informatycznych. Organizacje, które chcą wdrożyć systemy informacyjne, są zachęcane do przeprowadzenia szerokiej oceny wymagań, z uwzględnieniem potrzeb operacyjnych każdego interesariusza systemu.

Informacje zawarte w rozdziale 4 niniejszego tomu zawierają szczegóły architektury, które umożliwiają zrozumienie możliwości operacyjnych przykładowego rozwiązania. Wytyczne są również zawarte w normach, np. Międzynarodowej Organizacji Normalizacyjnej (*ang. International Organization for Standardization – ISO*), Międzynarodowej Komisji Elektrotechnicznej (*ang. International Electrotechnical Commission – IEC*), Instytucie Inżynierów Elektryków i Elektroników (*ang. Institute of Electrical and Electronics Engineers – IEEE*) 15288:2015, *Systems and software engineering-System life cycle processes* [15]; oraz publikacji NIST SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [16], które dostarczają wskazówek w tym zakresie. Dzięki tym normom organizacje mogą zdecydować się na przyjęcie tylko tych części, które są istotne dla ich środowiska i kontekstu biznesowego.

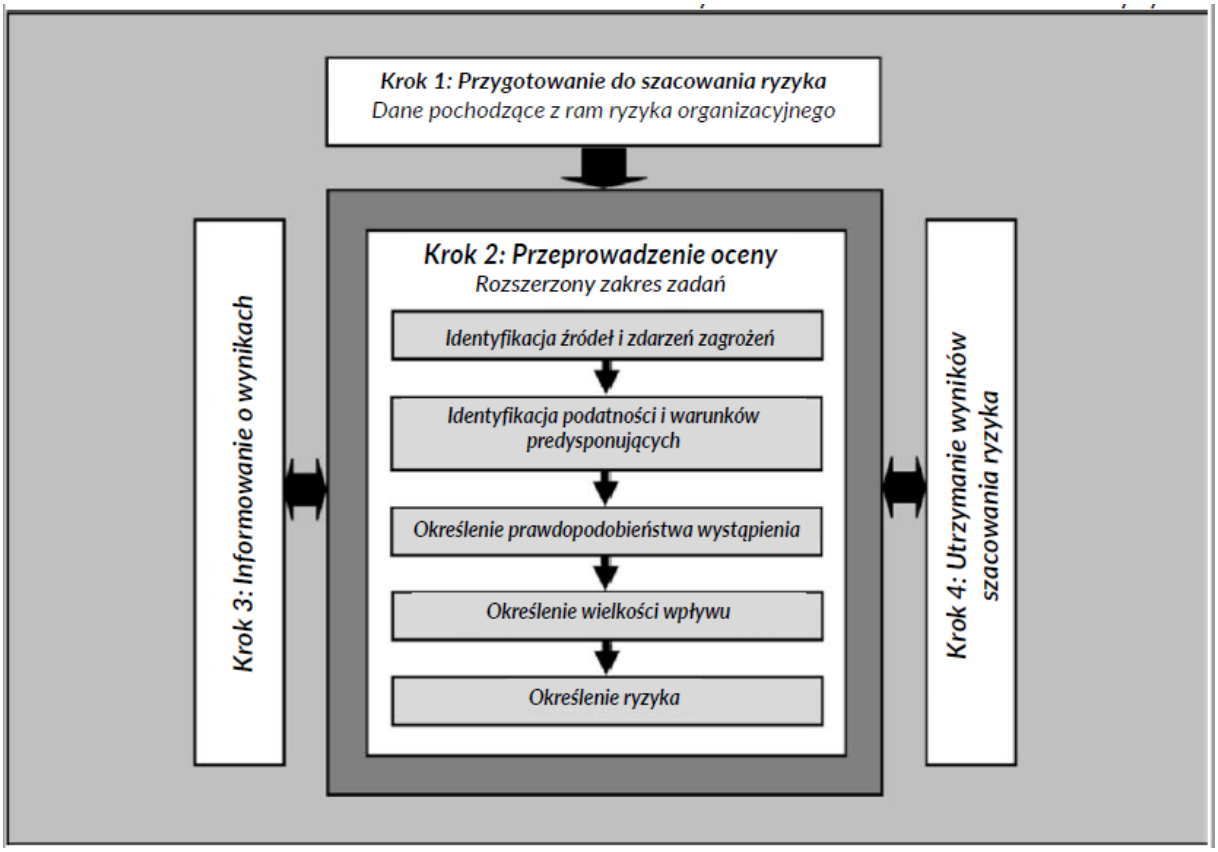
3.4. SZACOWANIE RYZYKA

W publikacji NIST SP 800-30 w wersji 1, *Guide for Conducting Risk Assessments* [12], stwierdza się, że ryzyko jest „miarą stopnia, w jakim podmiot jest zagrożony przez potencjalne okoliczności lub zdarzenia, i zazwyczaj jest funkcją: (I) niekorzystnych skutków, które powstałyby w przypadku wystąpienia okoliczności lub zdarzenia oraz (II) prawdopodobieństwa ich wystąpienia". W dalszej części przewodnika zdefiniujemy szacowania ryzyka jako „proces identyfikacji, szacowania i nadawania priorytetu zagrożeniom dla działalności organizacji (w tym misji, funkcji, wizerunku, reputacji), aktywów organizacji, osób fizycznych, innych organizacji i państwa, wynikających z działania systemu informacyjnego. Część dotycząca zarządzania ryzykiem, obejmuje analizy zagrożeń i podatności na zagrożenia oraz uwzględnia środki zaradcze w postaci planowanych lub wprowadzonych zabezpieczeń".

NCCoE zaleca, aby wszelkie dyskusje na temat zarządzania ryzykiem, szczególnie na poziomie organizacji, rozpoczynały się od kompleksowego zapoznania się z publikacją NIST SP 800-37[5] w wersji 2, *Risk Management Framework for Information Systems and Organizations* [17] – materiałem, który jest dostępny publicznie. Wytyczne ram zarządzania ryzykiem (*ang. Risk Management Framework – RMF*) [8], jako całość, okazały się nieocenione, dając nam punkt odniesienia do oszacowania ryzyka, na podstawie którego opracowaliśmy projekt, charakterystykę bezpieczeństwa rozwiązania i niniejszy przewodnik.

Niniejszy punkt zawiera informacje na temat procesu szacowania ryzyka zastosowanego w celu poprawy stanu bezpieczeństwa urządzeń mobilnych organizacji Orvilia Development. Zazwyczaj szacowanie ryzyka oparte na publikacji NIST SP 800-30 w wersji 1 przebiega zgodnie z czteroetapowym procesem przedstawionym na rysunku 3-2: Przygotowanie do oceny, przeprowadzenie oceny, informowanie o wynikach i utrzymanie oceny. Szczegółowe informacje na temat oceny ryzyka można znaleźć w załączniku F.

[5] Polskojęzyczna publikacja NSC 800-37.



Rysunek 3-2 Proces szacowania ryzyka

Celem szacowania ryzyka dla Orvilia Development jest zidentyfikowanie i udokumentowanie zmian w misji firmy mających wpływ na ryzyko, wynikających z jej nowego statusu jako kontrahenta agencji rządowych i wdrożenia urządzeń mobilnych COPE.

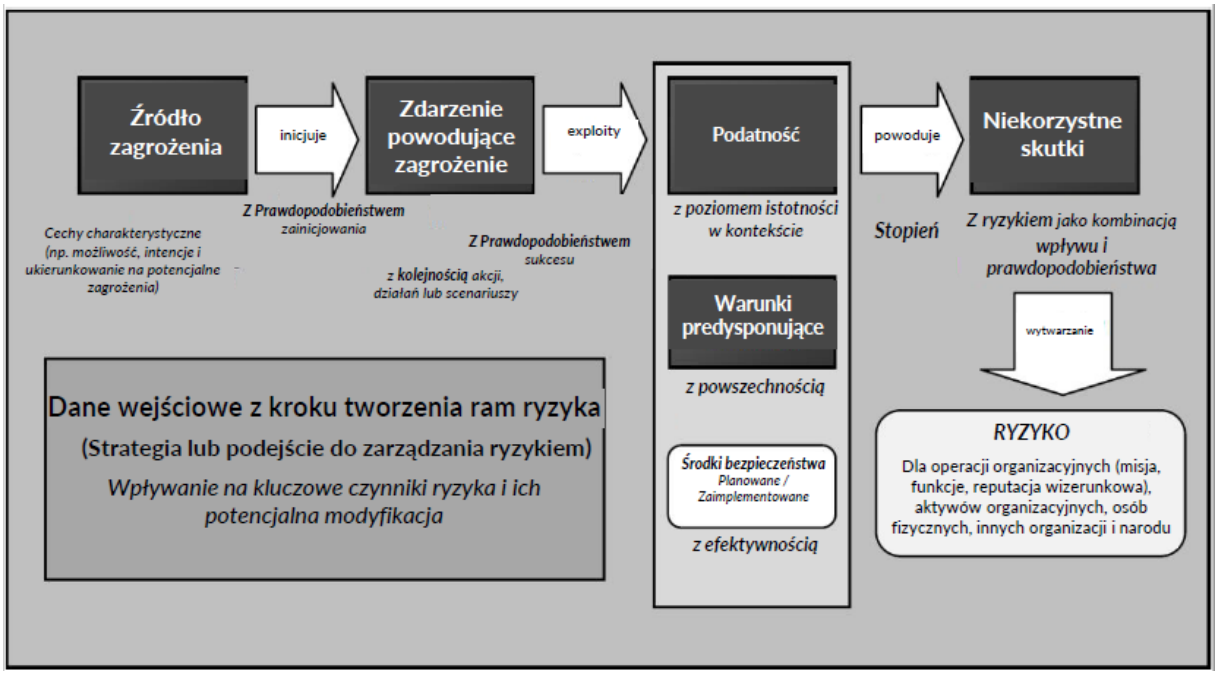
3.4.1. SZACOWANIE RYZYKA W FIKCYJNEJ ORGANIZACJI ORVILIA DEVELOPMENT

Niniejsza ocena ryzyka obejmuje mobilne wdrożenie w Orvilia, na które składają się urządzenia mobilne używane do uzyskiwania dostępu do zasobów przedsiębiorstwa wraz z wszelkimi komponentami zaplecza (*ang. backend*) IT używanymi do zarządzania tymi urządzeniami mobilnymi lub zapewniania im określonych usług.

Założenia i ograniczenia szacowania ryzyka zostały opracowane przy użyciu ogólnego modelu ryzyka z publikacji NIST SP 800-30 w wersji 1, jak pokazano na rysunku 3-3,

w celu zidentyfikowania następujących niezbędnych elementów szacowania ryzyka:

- źródła zagrożeń
- zdarzenia powodujące zagrożenie
- podatności
- warunki predysponujące
- środki bezpieczeństwa
- niekorzystne skutki
- ryzyko organizacyjne



Rysunek 3-3 Ogólny model ryzyka z publikacji NIST 800-30

3.4.2. OPRACOWYWANIE OPISÓW ZDARZEŃ POWODUJĄCYCH ZAGROŻENIE

W ramach projektu Orvilia przeanalizowano przykładowe tabele zawarte w publikacji NIST SP 800-30 w wersji 1 – tabelę F-1, tabelę F-2, tabelę F-3, tabelę F-4 i tabelę F-5—oraz zbadano źródła zagrożeń dla urządzeń mobilnych.

Korzystając z tego procesu, kierownictwo Orvilia zidentyfikowało potencjalne zagrożenia dla urządzeń mobilnych, które opisano w poniższych punktach. Zestawienie zdarzeń powodujących zagrożenia uwzględnionych w przykładowym rozwiązaniu z tego przewodnika i odpowiadających im pozycji z katalogu zagrożeń dla urządzeń mobilnych można znaleźć w tabeli 3-1.

Uwaga dotycząca wyboru zdarzeń powodujących zagrożenie: Zdarzenia te zostały opracowane poprzez określenie zagrożeń, które mogłyby znacząco zakłócić przebieg procesów organizacji Orvilia, na podstawie katalogu zagrożeń dla urządzeń mobilnych NIST [9]. W trosce o zwięzłość ograniczyliśmy liczbę zidentyfikowanych zagrożeń do tych, co do których istniało przypuszczenie, że prawdopodobieństwo ich wystąpienia i ich negatywnych skutków w konkretnym scenariuszu organizacji Orvilia jest wysokie. Zagrożenia z katalogu zagrożeń dla urządzeń mobilnych NIST, które mogły mieć mniejszy wpływ na organizację Orvilia, nie były na tyle istotne, aby stać się częścią poniższych 12 zdarzeń powodujących zagrożenia, które uznano za priorytetowe i uwzględniono w architekturze bezpieczeństwa urządzeń mobilnych.

Tabela 3-1 Zestawienie zdarzeń powodujących zagrożenia z odpowiadającymi im pozycjami w katalogu zagrożeń dla urządzeń mobilnych

Zdarzenie powodujące zagrożenie (*ang. Threat Event – TE*)	Identyfikator zagrożenia z katalogu zagrożeń dla urządzeń mobilnych NIST
TE-1	APP-2, APP-12
TE-2	AUT-9
TE-3	APP-5, AUT-10, APP-31, APP-40, APP-32, APP-2
TE-4	STA-9, APP-4, STA-16, STA-0, APP-26
TE-5	APP-32, APP-36
TE-6	STA-7, EMM-3
TE-7	CEL-18, APP-0, LPN-2

Zdarzenie powodujące zagrożenie (*ang. Threat Event – TE*)	Identyfikator zagrożenia z katalogu zagrożeń dla urządzeń mobilnych NIST
TE-8	AUT-2, AUT-4
TE-9	APP-9, AUT-0
TE-10	EMM-5
TE-11	PHY-0
TE-12	EMM-9

3.4.2.1. ZDARZENIE POWODUJĄCE ZAGROŻENIE 1 — NIEAUTORYZOWANY DOSTĘP DO WRAŻLIWYCH INFORMACJI ZA POŚREDNICTWEM ZŁOŚLIWEJ APLIKACJI LUB APLIKACJI NARUSZAJĄCEJ PRYWATNOŚĆ

Podsumowanie: Aplikacja mobilna może służyć do prób gromadzenia i eksfiltracji wszelkich danych, do których uzyskała dostęp. Obejmuje to wszelkie informacje generowane podczas korzystania z aplikacji (np. dane wejściowe wprowadzane przez użytkownika), przyznane przez niego uprawnienia (np. dostęp do kontaktów, kalendarza, dzienników połączeń, rolki z aparatu) oraz ogólne dane urządzenia dostępne dla dowolnej aplikacji (np. międzynarodowy identyfikator urządzenia mobilnego, marka i model urządzenia, numer seryjny). Co więcej, jeśli złośliwa aplikacja wykorzysta lukę w innych programach, systemie operacyjnym (*ang. operating system – OS*) lub oprogramowaniu układowym urządzenia, aby doprowadzić do eskalacji uprawnień, może uzyskać nieautoryzowany dostęp do wszelkich danych przechowywanych na urządzeniu lub w inny sposób dostępnych za jego pośrednictwem.

Analiza szacowanego ryzyka:

Ogólne prawdopodobieństwo: Bardzo wysokie

Uzasadnienie: Pracownicy mogą pobierać dowolne aplikacje w dowolnym momencie. Jeśli pracownik potrzebuje aplikacji, która zapewnia pożądaną funkcję, może pobrać ją z dowolnego dostępnego źródła (zaufanego lub niezaufanego). Jeśli aplikacja obsługuje

pożądaną przez pracownika funkcję, może on pobrać aplikację z niezaufanego źródła, w którym aplikacje wymagają uprawnień naruszających prywatność.

Poziom wpływu: Wysoki

Uzasadnienie: Urządzenia mobilne organizacji Orvilia mają obecnie możliwość pobrania aplikacji z niezaufanego źródła, w którym aplikacje wymagają uprawnień naruszających prywatność. Stanowi to zagrożenie dla wrażliwych danych firmy, ponieważ niektóre aplikacje mogą zawierać funkcje umożliwiające dostęp do danych firmowych bez wiedzy użytkownika.

3.4.2.2. ZDARZENIE POWODUJĄCE ZAGROŻENIE 2 — KRADZIEŻ DANYCH UWIERZYTELNIAJĄCYCH ZA POŚREDNICTWEM USŁUGI KRÓTKICH WIADOMOŚCI TEKSTOWYCH (ANG. SHORT MESSAGE SERVICE – SMS) LUB KAMPANII E-MAIL SŁUŻĄCEJ DO WYŁUDZANIA INFORMACJI

Podsumowanie: Złośliwe podmioty mogą tworzyć fałszywe strony internetowe, które mają naśladować wygląd i działanie oficjalnych witryn i zachęcać użytkowników do uwierzytelnienia się na nich poprzez dystrybucję wiadomości za pośrednictwem usługi SMS lub poczty elektronicznej. Skuteczne wykorzystanie technik inżynierii społecznej, takich jak podszywanie się pod autorytet lub stwarzanie poczucia pilności, może skłonić użytkownika do rezygnacji z analizy wiadomości i przystąpienia do uwierzytelnienia na fałszywej stronie internetowej. Wprowadzone dane uwierzytelniające użytkownika są następnie przechwytywane i przechowywane, a następnie (zazwyczaj) przekazywane do prawdziwej strony internetowej w celu rozwiania podejrzeń.

Analiza szacowanego ryzyka:

Ogólne prawdopodobieństwo: Bardzo wysokie

Uzasadnienie: Kampanie wyłudzania informacji są powszechnym zagrożeniem, które pojawia się niemal codziennie.

Poziom wpływu: Wysoki

Uzasadnienie: Udana kampania wyłudzania informacji może zapewnić złośliwemu podmiotowi firmowe dane uwierzytelniające umożliwiające dostęp do wrażliwych danych

biznesowych lub osobiste dane uwierzytelniające, które mogą prowadzić do naruszenia bezpieczeństwa danych firmowych lub infrastruktury za pośrednictwem innych środków.

3.4.2.3. ZDARZENIE POWODUJĄCE ZAGROŻENIE 3 — ZŁOŚLIWE APLIKACJE INSTALOWANE ZA POŚREDNICTWEM ADRESÓW URL W WIADOMOŚCIACH SMS LUB E-MAIL

Podsumowanie: Złośliwe podmioty mogą wysyłać użytkownikom wiadomości SMS lub e-mail zawierające adres URL, pod którym hostowana jest złośliwa aplikacja. Zazwyczaj takie wiadomości są tworzone z wykorzystaniem technik inżynierii społecznej, które mają na celu zniechęcenie odbiorców do sprawdzenia charakteru wiadomości, zwiększając tym samym prawdopodobieństwo skorzystania z adresu URL za pomocą urządzenia mobilnego. Jeśli użytkownik to zrobi, dojdzie do próby pobrania i zainstalowania aplikacji. Skuteczne wykorzystanie socjotechniki przez atakującego może skłonić nawet ostrożnego użytkownika do udzielenia wszelkiego zaufania wymaganego przez twórcę i wszystkich uprawnień wymaganych przez aplikację. Udzielenie pierwszej zgody ułatwia instalację innych złośliwych aplikacji od tego samego twórcy, a przyznanie drugiej zwiększa potencjał aplikacji do wyrządzenia bezpośrednich szkód.

Analiza szacowanego ryzyka:

Ogólne prawdopodobieństwo: Wysokie

Uzasadnienie: Instalowanie złośliwych aplikacji za pośrednictwem adresów URL jest mniej powszechne niż inne próby wyłudzenia informacji. Proces pobierania aplikacji lokalnie wymaga od użytkownika znacznie więcej zaangażowania i uwagi (np. zaufania do certyfikatu dewelopera) niż w przypadku standardowych prób wyłudzenia danych, które wymagają od niego jedynie podania nazwy użytkownika i hasła. Użytkownik może kontynuować proces pobierania lokalnie w celu uzyskania aplikacji o pożądanej funkcji.

Poziom wpływu: Wysoki

Uzasadnienie: Zainstalowanie złośliwej aplikacji pobranej lokalnie przez użytkownika może zapewnić złośliwemu podmiotowi pełny dostęp do urządzenia mobilnego — a tym samym dostęp do danych firmowych i danych uwierzytelniających — bez wiedzy użytkownika.

3.4.2.4. ZDARZENIE POWODUJĄCE ZAGROŻENIE 4 – UTRATA POUFNOŚCI I INTEGRALNOŚCI W WYNIKU WYKORZYSTANIA ZNANEJ PODATNOŚCI W SYSTEMIE OPERACYJNYM LUB OPROGRAMOWANIU UKŁADOWYM

Podsumowanie: Gdy złośliwe oprogramowanie z powodzeniem wykorzystuje lukę w zabezpieczeniach mobilnego systemu operacyjnego lub sterowników urządzenia, wprowadzony kod jest zazwyczaj wykonywany z podwyższonymi uprawnieniami, a następnie wydaje polecenia z poziomu użytkownika głównego lub jądra systemu operacyjnego. Polecenia te mogą być wystarczające dla niektórych atakujących, aby osiągnąć swój cel, ale zaawansowane złośliwe podmioty zazwyczaj próbują zainstalować dodatkowe złośliwe narzędzia i pozostać na stałe. W przypadku powodzenia złośliwy podmiot będzie mógł przeprowadzać dalsze ataki na użytkownika, urządzenie lub inne systemy podłączone do urządzenia. W rezultacie wszelkie dane przechowywane na urządzeniu, generowane przez nie lub dostępne za jego pośrednictwem w tym czasie lub w przyszłości mogą zostać naruszone.

Analiza szacowanego ryzyka:

Ogólne prawdopodobieństwo: Wysokie

Uzasadnienie: w rezultacie bezpieczeństwo wszelkich danych przechowywanych na urządzeniu, generowanych przez nie lub dostępnych za jego pośrednictwem w tym czasie lub w przyszłości może zostać naruszone. Użytkownicy wykonują *jailbreak* urządzeń z systemem iOS i rootują urządzenia z systemem Android, aby pobierać aplikacje innych firm i stosować unikalne ustawienia/konfiguracje, których normalnie nie da się zastosować na urządzeniu lub uzyskać dostępu do nich.

Poziom wpływu: Wysoki

Uzasadnienie: Wykorzystanie luki w zabezpieczeniach umożliwia obejście środków bezpieczeństwa i modyfikację chronionych danych urządzenia, które nie powinny być zmieniane. W przypadku urządzeń po *jailbreaku* lub rootowaniu istnieje możliwość wykorzystania luk w zabezpieczeniach jądra i zezwolenia zewnętrznym aplikacjom/usługom na dostęp z uprawnieniami głównego użytkownika, który może być również wykorzystany do ominięcia zabezpieczeń wbudowanych lub zastosowanych na urządzeniu mobilnym.

3.4.2.5. ZDARZENIE POWODUJĄCE ZAGROŻENIE 5 — NARUSZENIE PRYWATNOŚCI POPRZEZ NIEWŁAŚCIWE WYKORZYSTANIE CZUJNIKÓW URZĄDZENIA

Podsumowanie: Złośliwe podmioty z dostępem (autoryzowanym lub nieautoryzowanym) do czujników urządzenia (mikrofonu, kamery, żyroskopu, odbiornika globalnego systemu pozycjonowania (*ang. Global Positioning System – GPS*) i radia) mogą wykorzystywać je do prowadzenia inwigilacji. Może ona być skierowana przeciwko użytkownikowi, jak w przypadku śledzenia lokalizacji urządzenia, lub może być stosowana bardziej ogólnie, np. poprzez nagrywanie dźwięków w pobliżu. Dane przechwycone przez czujniki mogą być natychmiast użyteczne dla złośliwego podmiotu — na przykład nagranie ze spotkania kierownictwa. Dane mogą być również analizowane oddzielnie lub w połączeniu z innymi danymi w celu uzyskania wrażliwych informacji. Na przykład, nagrania audio aktywności na urządzeniu lub w jego pobliżu mogą być wykorzystane do probabilistycznego określenia danych wejściowych wprowadzanych przez użytkownika na ekranach dotykowych i klawiaturach – praktycznie zmieniając urządzenie w zdalny rejestrator klawiszy.

Analiza szacowanego ryzyka:

Ogólne prawdopodobieństwo: Bardzo wysokie

Uzasadnienie: w przeszłości problem ten był obserwowany w publicznych sklepach z aplikacjami, gdzie rzekomo były one wykorzystywane do gromadzenia danych [18]. Jak wspomniano w zdarzeniu powodującym zagrożenie nr 1, pobrana aplikacja może bez wiedzy użytkownika uzyskać uprawnienia naruszające prywatność, które umożliwiają dostęp do czujników urządzenia.

Poziom wpływu: Wysoki

Uzasadnienie: Użytkownik może nie być świadomy niewłaściwego wykorzystywania czujników. Umożliwia to gromadzenie wrażliwych danych przedsiębiorstwa, takich jak lokalizacja, bez wiedzy użytkownika.

3.4.2.6. ZDARZENIE POWODUJĄCE ZAGROŻENIE 6 — NARUSZENIE INTEGRALNOŚCI URZĄDZENIA LUB JEGO KOMUNIKACJI SIECIOWEJ POPRZEZ INSTALACJĘ ZŁOŚLIWEGO SYSTEMU EMM/MDM, SIECI, PROFILI VPN LUB CERTYFIKATÓW.

Podsumowanie: Złośliwe podmioty, które pomyślnie zainstalują profil — sieciowy lub w wirtualnej sieci prywatnej (VPN) — lub certyfikat systemu do zarządzania urządzeniami mobilnymi w przedsiębiorstwie/zarządzania urządzeniami mobilnymi (*ang. Enterprise Mobility Management – EMM/Mobile Device Management – MDM*), uzyskają dodatkową kontrolę nad urządzeniem lub jego komunikacją. Obecność złośliwego profilu EMM/MDM umożliwi atakującemu nadużywanie istniejących interfejsów programistycznych aplikacji (*ang. application programming interfaces – API*) systemu operacyjnego w celu wysyłania do urządzenia szerokiej gamy poleceń. Może to umożliwić złośliwemu podmiotowi uzyskanie informacji o urządzeniu, instalowanie lub ograniczanie aplikacji albo zdalne lokalizowanie, blokowanie lub czyszczenie urządzenia. Złośliwe profile sieciowe mogą umożliwić złośliwemu podmiotowi automatyczne zmuszanie urządzenia do łączenia się z punktami dostępu znajdującymi się pod jego kontrolą w celu przeprowadzenia ataku typu „person-in-the-middle” na wszystkie połączenia wychodzące. Alternatywnie, złośliwe profile VPN mogą umożliwiać niewykrytą eksfiltrację wrażliwych danych poprzez ich szyfrowanie. Ukrywa je to przed narzędziami do skanowania sieci. Ponadto złośliwe certyfikaty mogą umożliwić złośliwemu podmiotowi zmuszenie urządzenia do automatycznego zaufania połączeniom ze złośliwymi serwerami internetowymi, bezprzewodowymi punktami dostępowymi lub instalacji aplikacji znajdujących się pod kontrolą atakującego.

Analiza szacowanego ryzyka:

Ogólne prawdopodobieństwo: Umiarkowane

Uzasadnienie: w przeciwieństwie do instalowania aplikacji, instalacja profilu sieciowego, VPN i certyfikatów systemu EMM/MDM wymaga od użytkownika dodatkowego wysiłku i zrozumienia w celu prawidłowego wdrożenia.

Poziom wpływu: Bardzo wysoki

Uzasadnienie: Jeśli złośliwy podmiot będzie w stanie zainstalować złośliwe profile konfiguracji lub certyfikaty, będzie mógł wykonywać takie działania, jak odszyfrowywanie ruchu sieciowego, a być może nawet kontrolować urządzenie.

3.4.2.7. ZDARZENIE POWODUJĄCE ZAGROŻENIE 7 — UTRATA POUFNOŚCI WRAŻLIWYCH INFORMACJI POPRZEZ PODSŁUCHIWANIE NIEZASZYFROWANEJ KOMUNIKACJI URZĄDZENIA

Podsumowanie: Złośliwe podmioty mogą z łatwością podsłuchiwać komunikację za pośrednictwem niezaszyfrowanych sieci bezprzewodowych, takich jak publiczne punkty dostępu Wi-Fi, które są powszechnie dostępne w kawiarniach i hotelach. Jeśli urządzenie jest podłączone do takiej sieci, złośliwy podmiot może uzyskać nieautoryzowany dostęp do wszelkich danych wysyłanych lub odbieranych przez urządzenie dla każdej sesji, która nie jest chroniona przez szyfrowanie w warstwie transportowej lub aplikacji. Nawet jeśli przesyłane dane zostały zaszyfrowane, osoba atakująca może mieć dostęp do domen, adresów protokołu internetowego (*ang. Internet Protocol – IP*) i usług (oznaczonych numerami portów), z którymi łączy się urządzenie. Takie informacje mogą zostać wykorzystane w przyszłych atakach typu *watering hole* lub *person-in-the-middle* na użytkownika urządzenia.

Ponadto wgląd w ruch w warstwie sieciowej umożliwia złośliwemu podmiotowi przeprowadzanie ataków bocznymi kanałami na zaszyfrowane wiadomości, co nadal może skutkować utratą poufności. Co więcej, podsłuchiwanie niezaszyfrowanych wiadomości podczas wykonywania protokołu uzgodnienia w celu ustanowienia zaszyfrowanej sesji z innym hostem lub punktem końcowym może ułatwić ataki, które ostatecznie zagrażają bezpieczeństwu sesji.

<u>Analiza szacowanego ryzyka:</u>

Ogólne prawdopodobieństwo: Wysokie

Uzasadnienie: Użytkownicy potrzebują dostępu do sieci, aby pobierać wiadomości e-mail i korzystać z usług w chmurze oraz innych niezbędnych danych w Internecie.

Użytkownicy mogą łączyć się z łatwo dostępnymi bezpłatnymi punktami dostępu do Internetu w miejscach publicznych, takich jak kawiarnie, hotele i lotniska.

Poziom wpływu: Wysoki

Uzasadnienie: Użytkownicy mogą łączyć się z niezaszyfrowanymi sieciami bezprzewodowymi, a wiele aplikacji nie szyfruje prawidłowo komunikacji sieciowej. Niewłaściwe stosowanie szyfrowania lub jego brak umożliwia złośliwym podmiotom podsłuchiwanie ruchu sieciowego.

3.4.2.8. ZDARZENIE POWODUJĄCE ZAGROŻENIE 8 — NARUSZENIE INTEGRALNOŚCI URZĄDZENIA POPRZEZ ZASTOSOWANIE KODU ODBLOKOWUJĄCEGO, KTÓRY ZOSTAŁ ZAOBSERWOWANY, WYWNIOSKOWANY LUB POZYSKANY NA DRODZE ATAKU SIŁOWEGO

Podsumowanie: Złośliwy podmiot może pozyskać kod odblokowujący urządzenie użytkownika poprzez jego bezpośrednią obserwację, atak kanałem bocznym lub atak siłowy. Aby zastosować pierwszą technikę, wystarczy zbliżyć się do urządzenia. Tylko trzecia technika wymaga fizycznego dostępu do niego. Jednak ataki bocznym kanałem, w którym kod odblokowujący uzyskuje się poprzez wywnioskowanie go z czynności dotykania i przeciągania palcem po ekranie, mogą być podejmowane przez aplikacje z dostępem do dowolnych urządzeń peryferyjnych wykrywających dźwięk lub ruch (mikrofon, żyroskop lub akcelerometr). Po uzyskaniu kodu odblokowującego urządzenie, złośliwy podmiot z fizycznym dostępem do niego uzyska natychmiastowy wgląd we wszelkie dane lub funkcje, które nie są chronione przez dodatkowe mechanizmy kontroli dostępu. Poza tym jeśli użytkownik używa kodu odblokowującego urządzenie jako danych uwierzytelniających do innych systemów, atakujący może uzyskać do nich nieautoryzowany dostęp.

Analiza szacowanego ryzyka:

Ogólne prawdopodobieństwo: Wysokie

Uzasadnienie: w przeciwieństwie do zaglądania przez ramię w celu zaobserwowania kodu użytkownika, ataki siłowe nie są tak powszechne lub skuteczne ze względu na wbudowane mechanizmy zapobiegawcze. Mechanizmy te obejmują narastający wykładniczo czas wyłączenia/blokady, a także wymazywanie pamięci urządzenia po określonej liczbie nieudanych prób odblokowania.

Poziom wpływu: Wysoki

Uzasadnienie: Jeśli złośliwy podmiot jest w stanie odblokować urządzenie bez zgody użytkownika, może mieć pełną kontrolę nad jego kontem firmowym, a tym samym uzyskać nieautoryzowany dostęp do danych firmowych.

3.4.2.9. ZDARZENIE POWODUJĄCE ZAGROŻENIE 9 — NIEAUTORYZOWANY DOSTĘP DO USŁUG ZAPLECZA POPRZEZ LUKI W UWIERZYTELNIANIU LUB PRZECHOWYWANIU DANYCH UWIERZYTELNIAJĄCYCH W WEWNĘTRZNIE OPRACOWANYCH APLIKACJACH

Podsumowanie: Jeśli złośliwy podmiot uzyska nieautoryzowany dostęp do urządzenia mobilnego, atakujący ma również dostęp do znajdujących się w nim danych i aplikacji. Urządzenie mobilne może zawierać wewnętrzne aplikacje organizacji, które dają dostęp do wrażliwych danych lub usług zaplecza (*ang. backend services*). Podatność ta może wynikać ze słabości lub luk w mechanizmach uwierzytelniania lub przechowywania danych uwierzytelniających zaimplementowanych w aplikacji wewnętrznej.

Analiza szacowanego ryzyka:

Ogólne prawdopodobieństwo: Bardzo wysokie

Uzasadnienie: Kod aplikacji zawiera często dane uwierzytelniające dla domyślnego hasła konta administratora. Domyślne hasła są łatwo dostępne w Internecie. Mogą one nie być zmieniane, aby umożliwić łatwy dostęp i wyeliminować presję związaną z koniecznością zapamiętywania hasła.

Poziom wpływu: Wysoki

Uzasadnienie: Udana próba pozyskania danych uwierzytelniających umożliwia atakującemu uzyskanie nieautoryzowanego dostępu do danych przedsiębiorstwa.

3.4.2.10. ZDARZENIE POWODUJĄCE ZAGROŻENIE 10 — NIEAUTORYZOWANY DOSTĘP DO ZASOBÓW PRZEDSIĘBIORSTWA Z URZĄDZENIA NIEZARZĄDZANEGO I NARAŻONEGO NA NARUSZENIE BEZPIECZEŃSTWA

Podsumowanie: Pracownik, który uzyskuje dostęp do zasobów przedsiębiorstwa z niezarządzanego urządzenia mobilnego, naraża organizację na skutki podatności, które mogą obejmować naruszenie bezpieczeństwa danych firmy. W przypadku urządzeń niezarządzanych nie są wykorzystywane mechanizmy bezpieczeństwa wdrożone przez organizację, takie jak ochrona przed zagrożeniami mobilnymi, analiza zagrożeń mobilnych, usługi weryfikacji aplikacji i zasady bezpieczeństwa mobilnego. W przypadku takich niezarządzanych urządzeń organizacja ma ograniczony wgląd w ich stan – również w sytuacji, gdy ich bezpieczeństwo zostanie naruszone przez złośliwy podmiot. W związku z tym użytkownicy, którzy naruszają zasady bezpieczeństwa w celu uzyskania nieautoryzowanego dostępu do zasobów przedsiębiorstwa z takich urządzeń, ryzykują umożliwienie atakującym dostępu do wrażliwych danych, usług i systemów organizacji.

Analiza szacowanego ryzyka:

Ogólne prawdopodobieństwo: Bardzo wysokie

Uzasadnienie: Może do tego dojść przypadkowo, gdy pracownik próbuje uzyskać dostęp do swojej poczty elektronicznej.

Poziom wpływu: Wysoki

Uzasadnienie: Niezarządzane urządzenia stanowią poważne zagrożenie dla bezpieczeństwa, ponieważ przedsiębiorstwo nie ma wglądu w stan ich zabezpieczeń i związane z nimi ryzyko. Dlatego zainfekowane urządzenie może umożliwić atakującemu próbę eksfiltracji wrażliwych danych przedsiębiorstwa.

3.4.2.11. ZDARZENIE POWODUJĄCE ZAGROŻENIE 11 — UTRATA DANYCH ORGANIZACJI Z POWODU ZGUBIENIA LUB KRADZIEŻY URZĄDZENIA

Podsumowanie: Ze względu na niewielkie rozmiary urządzeń mobilnych, mogą one zostać zgubione lub skradzione. Złośliwy podmiot, który uzyska fizyczną kontrolę nad

urządzeniem z nieodpowiednimi zabezpieczeniami, może uzyskać nieautoryzowany dostęp do wrażliwych danych lub zasobów dostępnych dla tego urządzenia.

Analiza szacowanego ryzyka:

Ogólne prawdopodobieństwo: Bardzo wysokie

Uzasadnienie: Urządzenia mobilne są małe i można je zgubić. Urządzenia firmowe mogą być gubione lub kradzione równie często jak urządzenia osobiste.

Poziom wpływu: Wysoki

Uzasadnienie: Podobnie jak w przypadku zdarzenia powodującego zagrożenie nr 9, jeśli złośliwy podmiot uzyska dostęp do urządzenia, może również zyskać dostęp do wrażliwych danych firmowych.

3.4.2.12. ZDARZENIE POWODUJĄCE ZAGROŻENIE 11 — UTRATA POUFNOŚCI DANYCH ORGANIZACJI Z POWODU ICH NIEAUTORYZOWANEGO PRZECHOWYWANIA W USŁUGACH NIEZARZĄDZANYCH PRZEZ ORGANIZACJĘ

Podsumowanie: Jeśli pracownik naruszy zasady zarządzania danymi, korzystając z niezarządzanych usług do przechowywania wrażliwych danych organizacji, dane te znajdą się poza jej kontrolą i nie będzie ona już w stanie chronić ich poufności, integralności ani dostępności. Złośliwe podmioty, które naruszą bezpieczeństwo nieautoryzowanego konta usługi lub dowolnego systemu obsługującego to konto, mogą uzyskać nieautoryzowany dostęp do danych.

Co więcej, przechowywanie wrażliwych danych w niezarządzanej usłudze może narazić użytkownika lub organizację na postępowanie sądowe za naruszenie obowiązujących przepisów (np. o eksporcie kryptografii) i może skomplikować działania organizacji mające na celu uzyskanie środków zaradczych lub naprawienie wszelkich przyszłych strat, takich jak te wynikające z publicznego ujawnienia tajemnic handlowych.

Analiza szacowanego ryzyka:

Ogólne prawdopodobieństwo: Wysokie

Uzasadnienie: Może to mieć miejsce zarówno celowo, jak i przypadkowo (np. poprzez wykonanie zrzutu ekranu i zapisanie kopii zapasowej zdjęcia w niezarządzanej usłudze w chmurze).

Poziom wpływu: Wysoki

Uzasadnienie: Przechowywanie danych w niezarządzanych usługach stanowi ryzyko dla poufności i dostępności danych firmowych, ponieważ przedsiębiorstwo traci nad nimi kontrolę.

3.4.3. IDENTYFIKACJA PODATNOŚCI I WARUNKÓW PREDYSPONUJĄCYCH

W punkcie 3.4 określono podatności i warunki predysponujące, które zwiększają prawdopodobieństwo, że zidentyfikowane zagrożenia będą miały negatywny wpływ na Orvilia Development. Wszystkie podatności lub warunki predysponujące zostały wymienione w tabeli 3-2 wraz z odpowiadającymi im zdarzeniami powodującymi zagrożenie i oceną ich powszechności. Więcej szczegółowych informacji na temat korzystania z ocen zdarzeń powodujących zagrożenie można znaleźć w załączniku F.

Tabela 3-2 Identyfikacja podatności i warunków predysponujących

Identyfikator podatności	Podatność lub warunek predysponujący	Wynikowe zdarzenia powodujące zagrożenie	Powszechność
VULN-1	Dostęp do poczty elektronicznej i innych zasobów przedsiębiorstwa jest możliwy z dowolnego miejsca, a wymagane jest jedynie uwierzytelnienie za pomocą nazwy użytkownika/hasła.	TE-2, TE-10, TE11	Bardzo duża
VULN-2	Pracownicy regularnie korzystają z publicznych sieci Wi-Fi w celu nawiązania zdalnej łączności z firmowych urządzeń mobilnych.	TE-7	Bardzo duża
VULN-3	Nie wdrożono systemu EMM/MDM, aby egzekwować i monitorować zgodność z zasadami bezpieczeństwa dotyczącymi firmowych urządzeń mobilnych.	TE-1, TE-3, TE-4, TE-5, TE-6, TE-7, TE-8, TE-9, TE-11, TE-12	Bardzo duża

3.4.4. PODSUMOWANIE WYNIKÓW SZACOWANIA RYZYKA

W tabeli 3-3 podsumowano wyniki szacowania ryzyka. Więcej szczegółowych informacji na temat metodologii zastosowanej do oceny ogólnego prawdopodobieństwa, poziomu skutków i ryzyka można znaleźć w załączniku F.

Tabela 3-3 Podsumowanie wyników szacowania ryzyka

Zdarzenie powodujące zagrożenie	Podatności, warunki predysponujące	Ogólne prawdopodobieństwo	Poziom wpływu	Ryzyko
TE-1: Nieautoryzowany dostęp do wrażliwych informacji za pośrednictwem złośliwej lub naruszającej prywatność aplikacji	VULN-3	Bardzo duże	Wysoki	Wysokie
TE-2: Kradzież danych uwierzytelniających poprzez kampanię wyłudzania informacji za pośrednictwem wiadomości SMS lub e-mail	VULN-1	Bardzo duże	Wysoki	Wysokie
TE-3: Złośliwe aplikacje zainstalowane za pośrednictwem adresów URL w wiadomościach SMS lub e-mail	VULN-3	Duże	Wysoki	Wysokie
TE-4: Utrata poufności i integralności w wyniku wykorzystania znanej podatności w systemie operacyjnym lub oprogramowaniu układowym	VULN-3	Duże	Wysoki	Wysokie
TE-5: Naruszenie prywatności poprzez niewłaściwe wykorzystanie czujników urządzenia	VULN-3	Bardzo duże	Wysoki	Wysokie

Zdarzenie powodujące zagrożenie	Podatności, warunki predysponujące	Ogólne prawdopodobieństwo	Poziom wpływu	Ryzyko
TE-6: Naruszenie integralności urządzenia lub jego komunikacji sieciowej poprzez instalację złośliwego systemu EMM/MDM, sieci, profili VPN lub certyfikatów.	VULN-3	Umiarkowane	Bardzo wysoki	Wysokie
TE-7: Utrata poufności wrażliwych informacji poprzez podsłuchiwanie niezaszyfrowanej komunikacji urządzenia	VULN-2, VULN-3	Duże	Wysoki	Wysokie
TE-8: Naruszenie integralności urządzenia poprzez zastosowanie kodu odblokowującego, który został zaobserwowany, wywnioskowany lub pozyskany na drodze ataku siłowego	VULN-3	Duże	Wysoki	Wysokie
TE-9: Nieautoryzowany dostęp do usług zaplecza poprzez luki w uwierzytelnianiu lub przechowywaniu danych uwierzytelniających w wewnętrznie opracowanych aplikacjach	VULN-3	Bardzo duże	Wysoki	Wysokie
TE-10: Nieautoryzowany dostęp do zasobów przedsiębiorstwa z urządzenia niezarządzanego i narażonego na naruszenie bezpieczeństwa	VULN-1	Bardzo duże	Wysoki	Wysokie
TE-11: Utrata danych organizacji z powodu zgubienia lub kradzieży urządzenia	VULN-1, VULN-3	Bardzo duże	Wysoki	Wysokie

Zdarzenie powodujące zagrożenie	Podatności, warunki predysponujące	Ogólne prawdopodobieństwo	Poziom wpływu	Ryzyko
TE-12: Utrata poufności danych organizacji z powodu ich nieautoryzowanego przechowywania w usługach niezarządzanych przez organizację	VULN-3	Duże	Wysoki	Wysokie

Uwaga 1: Ryzyko jest określane jakościowo w oparciu o skalę w tabeli I-2 załącznika I w publikacji specjalnej NIST 800-30 w wersji 1 [12].

Uwaga 2: Sama ocena ryzyka jest określana na podstawie zarówno ogólnego prawdopodobieństwa, jak i poziomu oddziaływania przy użyciu tabeli I2 w załączniku i do publikacji specjalnej NIST 800-30 w wersji 1 [12]. Ponieważ skale te nie są prawdziwymi skalami interwałowymi, łączne ogólne oceny ryzyka z tabeli I-2 nie zawsze dokładnie odpowiadają matematycznej średniej tych dwóch zmiennych. Widać to w powyższej tabeli, gdzie poziomy umiarkowane są ważniejsze niż inne oceny.

Uwaga 3: Oceny ryzyka odnoszą się do prawdopodobieństwa i poziomu niekorzystnego wpływu na działalność organizacji, jej aktywa, osoby fizyczne, inne organizacje lub państwo. Zgodnie z publikacją NIST SP 800-30 w wersji 1, negatywne skutki (i związane z nimi ryzyko) wahają się od nieistotnych (tj. bardzo niskie ryzyko), ograniczonych (niskie), poważnych (umiarkowane), dotkliwych lub katastrofalnych (wysokie), do wielu dotkliwych lub katastrofalnych skutków (bardzo wysokie).

3.4.5. SZACOWANIE RYZYKA DLA PRYWATNOŚCI

W tym punkcie opisano szacowanie ryzyka dla prywatności przeprowadzane w odniesieniu do architektury bezpieczeństwa przedsiębiorstwa Orvilia. Do przeprowadzenia szacowania ryzyka dla prywatności wykorzystano metodologię szacowania ryzyka dla prywatności (*ang. Privacy Risk Assessment Methodology – PRAM*) NIST. PRAM jest narzędziem do analizy, oceny i nadawania priorytetów zagrożeniom dla prywatności, które umożliwia organizacjom określenie sposobu reagowania i wybór odpowiednich rozwiązań. PRAM może również służyć jako użyteczne narzędzie

komunikacyjne do informowania o zagrożeniach dla prywatności w organizacji. Pusta wersja PRAM jest dostępna do pobrania na stronie internetowej NIST [19].

Do analizy problematycznych działań związanych z danymi w ramach PRAM wykorzystywany jest model ryzyka dla prywatności i cele inżynierii prywatności opisane w raporcie wewnętrznym NIST IR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [20]. Działania na danych to wszelkie operacje systemowe, w ramach których przetwarzane są dane osobowe. Przetwarzanie może obejmować gromadzenie, przechowywanie, rejestrowanie, analizowanie, generowanie, przekształcanie lub łączenie, ujawnianie, przekazywanie i usuwanie danych osobowych. Problematyczne działanie na danych to takie, które może mieć niekorzystny wpływ na konkretne osoby. W ramach działań PRAM zidentyfikowano poniższe potencjalne problemy dla osób fizycznych.

3.4.5.1. POTENCJALNE PROBLEMY DLA OSÓB FIZYCZNYCH

W ramach PRAM zidentyfikowano trzy działania na danych, które mogą stwarzać problemy dla osób fizycznych. Poniżej przedstawiono te trzy działania na danych wraz z analizą szacowanego ryzyka:

- blokowanie dostępu i wymazywanie pamięci urządzeń
- monitorowanie pracowników
- udostępnianie danych między stronami

3.4.5.1.1. DZIAŁANIE NA DANYCH 1: BLOKOWANIE DOSTĘPU I WYMAZYWANIE PAMIĘCI URZĄDZEŃ

Pracownicy najprawdopodobniej używają swoich urządzeń zarówno do celów osobistych, jak i związanych z pracą. Dlatego, jeśli system ma możliwość całkowitego wymazania pamięci urządzenia, może dojść do utraty osobistych danych przez pracowników. Jest to potencjalny problem dla osób fizycznych, ponieważ korzystanie przez pracowników z urządzeń służbowych zarówno do celów osobistych, jak i związanych z pracą jest powszechne.

W przypadku urządzeń, które mogą stanowić zagrożenie dla bezpieczeństwa organizacji, można zablokować dostęp do zasobów przedsiębiorstwa lub wymazać ich pamięć

i przywrócić ustawienia fabryczne, co może skutkować utratą informacji zawartych na urządzeniu. Potencjalne opcje minimalizacji skutków dla pracownika obejmują:

- zablokowanie dostępu urządzenia do zasobów przedsiębiorstwa do czasu ponownego przyznania uprawnień dostępu;
- selektywne wymazywanie elementów pamięci urządzenia bez usuwania wszystkich znajdujących się na nim danych; w przykładowym rozwiązaniu opcja ta jest dostępna dla urządzeń z systemem iOS;
- zalecanie pracownikom tworzenia kopii zapasowych osobistych danych przechowywanych na urządzeniach;
- ograniczenie pracownikom możliwości wymazywania danych lub blokowania dostępu.

3.4.5.1.2. DZIAŁANIE NA DANYCH 2: MONITOROWANIE PRACOWNIKÓW

Pracownicy mogą nie być świadomi monitorowania ich interakcji z systemem i mogą nie chcieć, aby takie monitorowanie miało miejsce. W sieciach należących do pracodawców lub przez nich kontrolowanych, takich jak w organizacji Orvilia, często monitoruje się aktywność, a w wielu przypadkach robi się to regularnie.

Oceniana infrastruktura umożliwia firmie Orvilia korzystanie z szeregu funkcji bezpieczeństwa, w tym z kompleksowego monitorowania. Znaczna ilość danych dotyczących pracowników, ich urządzeń i działań jest gromadzona i analizowana przez wiele stron. Potencjalne opcje minimalizacji skutków dla pracownika obejmują:

- ograniczenie możliwości przeglądania danych dotyczących pracowników i ich urządzeń przez personel;
- opracowanie zasad i technik organizacji mających na celu ograniczenie gromadzenia określonych elementów danych;
- opracowanie zasad i technik organizacji dotyczących usuwania danych osobowych.

3.4.5.1.3. DZIAŁANIE NA DANYCH 3: UDOSTĘPNIANIE DANYCH MIĘDZY STRONAMI

Przesyłanie danych o osobach i ich urządzeniach między różnymi stronami może być kłopotliwe dla pracowników, którzy mogą nie wiedzieć, kto ma dostęp do różnych informacji na ich temat.

Infrastruktura obejmuje kilka stron, które służą różnym celom wspierającym atrybuty bezpieczeństwa organizacji Orvilia. W związku z tym następuje znaczny przepływ danych dotyczących osób fizycznych i ich urządzeń między różnymi stronami.

Jeśli szerokie grono administratorów i współpracowników wie, którzy z członków personelu wykonują na swoich urządzeniach działania uruchamiające alerty bezpieczeństwa, może to prowadzić do niepożądanych skutków, takich jak poczucie wstydu pracowników. Potencjalne opcje minimalizacji skutków dla pracownika obejmują:

- opracowanie zasad i technik organizacji w zakresie anonimizacji danych;
- stosowanie szyfrowania;
- ograniczenie lub wyłączenie dostępu do danych;
- opracowanie zasad i technik organizacji mających na celu ograniczenie gromadzenia określonych elementów danych;
- korzystanie z umów w celu ograniczenia przetwarzania danych przez strony trzecie.

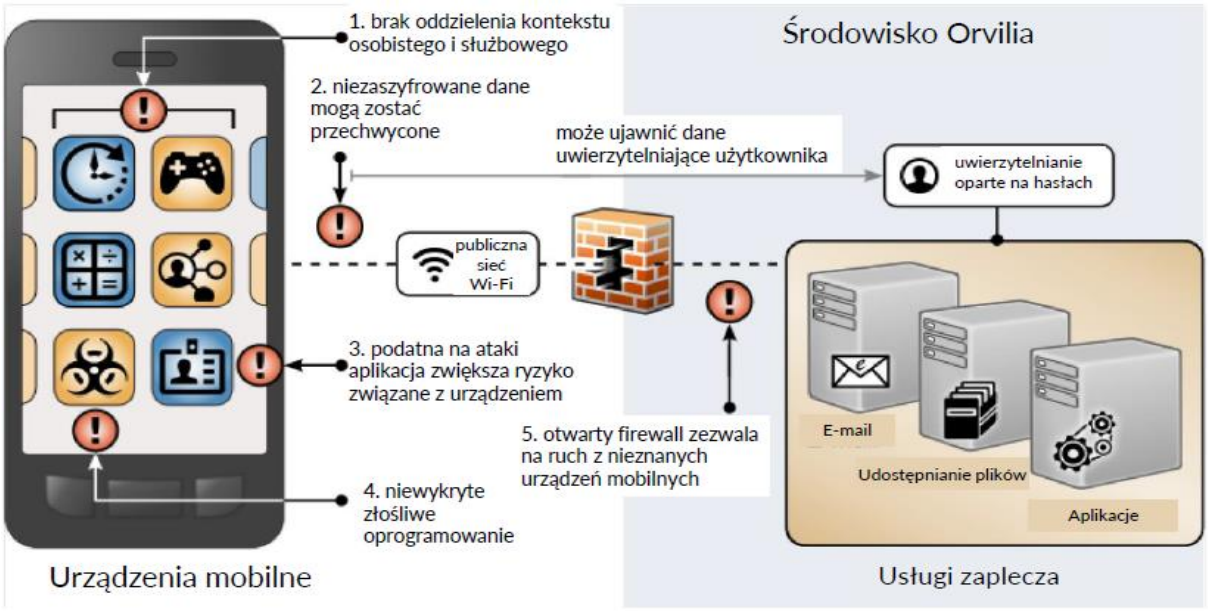
Dodatkowe informacje dotyczące takich potencjalnych problemów dla osób fizycznych i możliwych opcji zminimalizowania ich skutków dla pracowników znajdują się w załączniku G.

3.5. CELE ROZWIĄZANIA

W tym punkcie opisano cele rozwiązania dotyczące zmiany architektury zabezpieczeń urządzeń mobilnych w organizacji Orvilia. Poniżej znajduje się przegląd problemów związanych z bezpieczeństwem zidentyfikowanych w pierwotnej (zwanej również obecną) architekturze infrastruktury urządzeń mobilnych w Orvilia. Aby rozwiązać te problemy, opracowano listę celów bezpieczeństwa będącą ogólnym przeglądem czynników, które można zastosować w celu poprawy bezpieczeństwa architektury mobilnej w Orvilia.

3.5.1. PIERWOTNA ARCHITEKTURA

Przed zainwestowaniem w nowe zabezpieczenia swojej infrastruktury mobilnej, jak wynika z wyżej wspomnianej oceny ryzyka, Orvilia Development nie wdrożyła strategii bezpieczeństwa mobilnego. Zidentyfikowano kilka słabych punktów związanych z korzystaniem z urządzeń mobilnych. Podzbiór tych słabych punktów przedstawiono na rysunku 3-4.



Rysunek 3-4 Wdrożenie urządzeń mobilnych w organizacji Orvilia przed wprowadzeniem rozszerzonych zabezpieczeń

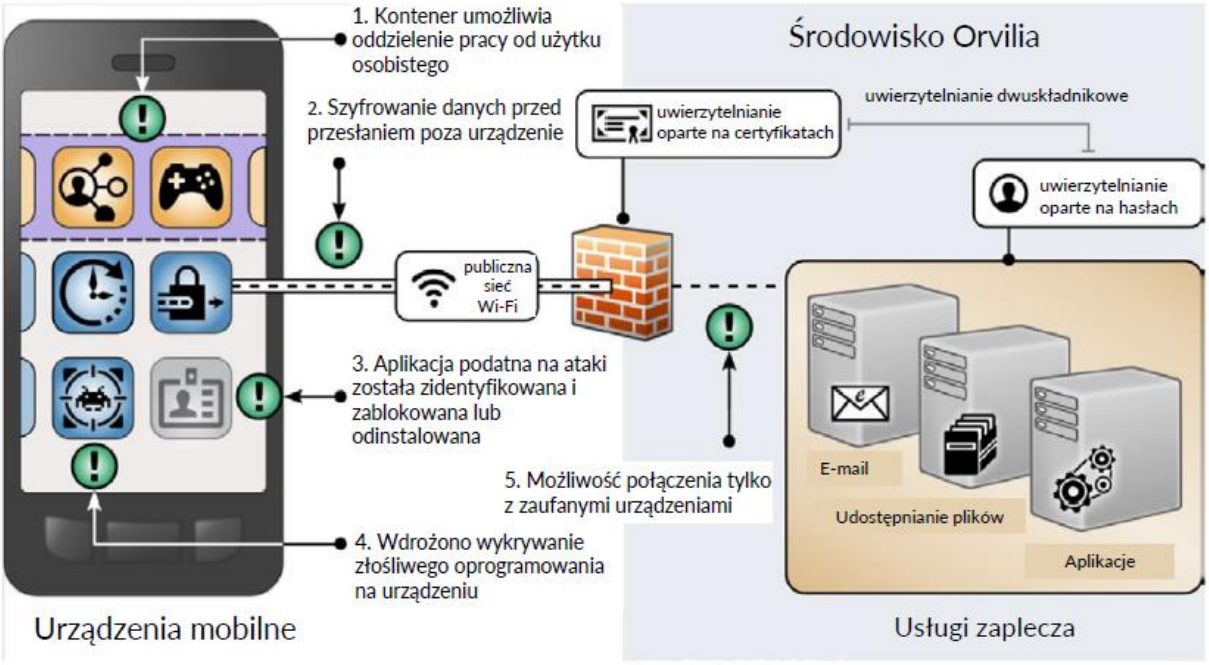
Na rysunku 3-4 czerwonym wykrzyknikiem oznaczono następujące problemy:

1. Dane organizacji i dane prywatne mogą zostać pomieszane, jeśli ta sama aplikacja jest używana do obu celów lub jeśli wiele aplikacji ma dostęp do wspólnych zasobów urządzenia (np. kontaktów lub kalendarza).
2. Urządzenia mobilne łączą się z siecią organizacji Orvilia z niezaszyfrowanych publicznych hotspotów Wi-Fi. Dane przesyłane przed nawiązaniem bezpiecznego połączenia, w tym hasła, są narażone na podsłuch.
3. Aplikacje do użytku służbowego lub osobistego mogą zawierać niezidentyfikowane luki lub podatności, które zwiększają ryzyko naruszenia bezpieczeństwa urządzenia.

4. Aplikacje mogą być pozyskiwane spoza oficjalnych sklepów, co zwiększa ryzyko, że są one złośliwym oprogramowaniem udającym bezpieczne programy.
5. Ponieważ urządzenia mobilne mogą łączyć się z nieznanych lokalizacji, reguły zapory muszą dopuszczać połączenia przychodzące z nierozpoznanych, potencjalnie złośliwych adresów IP.

3.5.2. CELE BEZPIECZEŃSTWA

Planując zwiększenie poziomu bezpieczeństwa obecnego wdrożenia, firma Orvilia zidentyfikowała ogólne cele w zakresie bezpieczeństwa, aby wyeliminować te niedociągnięcia, jak pokazano na rysunku 3-5.



Rysunek 3-5 Cele bezpieczeństwa organizacji Orvilia

Na rysunku 3-5 zielonym wykrzyknikiem oznaczono następujące strategie:

1. Informacje organizacji i dane osobiste można oddzielić, ograniczając przepływ danych między aplikacjami zarządzanymi i niezarządzanymi przez organizację. Wrażliwe dane są chronione przed przenoszeniem między kontekstem użytku służbowego i prywatnego.

2. Urządzenia mobilne mogą łączyć się z organizacją Orvilia za pośrednictwem sieci VPN lub podobnego rozwiązania w celu szyfrowania wszystkich danych przed ich przesłaniem z urządzenia, chroniąc w ten sposób niezaszyfrowane dane przed przechwyceniem.
3. Identyfikacja aplikacji z istotnymi lukami lub podatnościami ułatwia ich blokowanie lub odinstalowywanie z zarządzanych urządzeń, zmniejszając ryzyko dla organizacji.
4. W celu identyfikacji złośliwych aplikacji i ułatwienia ich usuwania na urządzeniach można wdrożyć funkcję wykrywania złośliwego oprogramowania.
5. Urządzenia mobilne mogą być wyposażone w certyfikat bezpieczeństwa, który umożliwia ich identyfikację i uwierzytelnianie w punkcie połączenia. W połączeniu z danymi uwierzytelniającymi użytkownika umożliwia to uwierzytelnianie dwuskładnikowe przy łączeniu się z urządzeń mobilnych.

Te ogólne cele, opracowane na podstawie przeglądu obecnego stanu bezpieczeństwa mobilnego, stanowią przykład tego, że gruntowny proces oceny ryzyka jest korzystny dla organizacji wdrażających zabezpieczenia urządzeń mobilnych.

3.6. TECHNOLOGIE

W tym punkcie opisano komponenty technologii specyficznej dla urządzeń mobilnych wykorzystywane w tym przykładowym rozwiązaniu. Technologie te zostały wybrane pod kątem celów bezpieczeństwa i zagrożeń zidentyfikowanych w ramach szacowania ryzyka. Ten punkt zawiera krótki opis każdej technologii i omówienie funkcji bezpieczeństwa, które każdy komponent zapewnia w celu rozwiązania problemów związanych z bezpieczeństwem organizacji Orvilia. Dodatkowe informacje znajdują się w załączniku I, w którym opisano technologie zastosowane w tym projekcie i przedstawiono zestawienie konkretnych zastosowanych produktów ze standardami cyberbezpieczeństwa i najlepszymi praktykami, z którymi zgodność produkty te zapewniają w przykładowym rozwiązaniu omówionym w niniejszym przewodniku.

3.6.1. KOMPONENTY ARCHITEKTURY

Komponenty bezpieczeństwa w tym punkcie są połączone w spójną architekturę, aby umożliwić przedsiębiorstwom przeciwdziałanie zagrożeniom dla bezpieczeństwa mobilnego i zapewnić bezpieczny dostęp do zasobów firmy z urządzeń mobilnych. Komponenty bezpieczeństwa opisane w tym punkcie zapewniają ochronę następujących komponentów architektury przedsiębiorstwa, do których użytkownicy z organizacji Orvilia uzyskują dostęp za pomocą swoich urządzeń mobilnych.

- E-mail/Outlook Web Access – kontakty
- Prywatny serwer czatu
- Obsługa podróży
- Intranet organizacji (np. wewnętrzne ogłoszenia, schematy organizacyjne, zasady)
- Raportowanie czasu pracy

3.6.1.1. ZAUFANE ŚRODOWISKO WYKONAWCZE

Zaufane środowisko wykonawcze (*ang. Trusted Execution Environment – TEE*) to „odporne na manipulacje środowisko przetwarzania, które działa w oparciu o oddzielne jądro. Gwarantuje ono autentyczność wykonywanego kodu, integralność stanów środowiska uruchomieniowego (np. rejestrów jednostki centralnej, pamięci i wrażliwych wejść/wyjść) oraz poufność kodu, danych i stanów środowiska uruchomieniowego przechowywanych w pamięci trwałej. Ponadto musi być w stanie zapewnić zdalne zaświadczenie, które udowodni jego wiarygodność dla stron trzecich” [21].

3.6.1.2. ZARZĄDZANIE MOBILNOŚCIĄ W PRZEDSIĘBIORSTWIE

Organizacje wykorzystują rozwiązania do zarządzania mobilnością w przedsiębiorstwie, aby zabezpieczyć urządzenia mobilne użytkowników, którzy są upoważnieni do dostępu do jej zasobów. Takie rozwiązania zazwyczaj składają się z dwóch głównych elementów. Pierwszym z nich jest usługa zaplecza, z której korzystają administratorzy urządzeń mobilnych do zarządzania zasadami, konfiguracjami i działaniami z zakresu

bezpieczeństwa stosowanymi dla zarejestrowanych urządzeń mobilnych. Drugim jest agent na urządzeniu, zwykle w formie aplikacji mobilnej, który integruje system operacyjny urządzenia z usługą zaplecza danego rozwiązania. Alternatywnie, system iOS może obsługiwać rejestrację w systemie EMM przez Internet.

Rozwiązanie EMM powinno co najmniej realizować funkcje systemu MDM, które obejmują możliwość dostarczania profili konfiguracji do urządzeń, egzekwowania na nich polityk bezpieczeństwa i monitorowania ich zgodności z tymi zasadami. Agent MDM na urządzeniu może zazwyczaj powiadamiać użytkownika urządzenia o wszelkich niezgodnych ustawieniach i może być w stanie automatycznie naprawić niektóre z nich. Organizacja może wykorzystywać dane dotyczące zgodności z polityką w celu informowania o swoich decyzjach dotyczących kontroli dostępu i przyznawać dostęp tylko urządzeniom, które wykazują wymagany poziom zgodności z obowiązującą polityką bezpieczeństwa.

Rozwiązania EMM zazwyczaj obejmują następujące elementy: zarządzanie aplikacjami mobilnymi, zarządzanie treściami mobilnymi oraz implementacje lub integracje z rozwiązaniami do konteneryzacji specyficznymi dla urządzenia lub mobilnego systemu operacyjnego, takimi jak Samsung Knox (więcej informacji można znaleźć w załączniku E). Funkcje te mogą być wykorzystywane do zarządzania instalacją i użytkowaniem aplikacji w oparciu o zaufanie do nich i ich przydatność do pracy. Ponadto mogą kontrolować sposób, w jaki zarządzane aplikacje uzyskują dostęp do danych organizacji i korzystają z nich, a także wzmacniać rozdział między osobistym i służbowym użytkowaniem urządzenia przez pracownika.

Co więcej, rozwiązania EMM często integrują się z różnorodnym zestawem dodatkowych narzędzi i technologii bezpieczeństwa, które zwiększają ich możliwości. Przykładem może być rozwiązanie EMM z wbudowanym narzędziem do ochrony przed zagrożeniami mobilnymi, które służy do wykrywania zagrożeń behawioralnych na urządzeniu i uruchamiania środków zaradczych bez konieczności komunikowania się z jakimkolwiek serwerem lub usługą poza urządzeniem. Ten rodzaj integracji umożliwia jednej aplikacji, agentowi EMM, zarządzanie urządzeniami, sieciami

i aplikacjami, ich wykrywanie i naprawianie, a także przeciwdziałanie atakom przy użyciu złośliwego oprogramowania i spersonalizowanego wyłudzania informacji. Dodatkowo środki zaradcze są autonomiczne na urządzeniu (nie wymagają połączenia z serwerem zasad), więc mają przewagę podczas przeciwdziałania sieciowym wektorom zagrożeń, takim jak podszywanie się typu Pineapple lub Stingray pod prawidłowe sieci Wi-Fi lub komórkowe [22].

Dodatkowe informacje na temat zarządzania urządzeniami mobilnymi za pomocą rozwiązań EMM można znaleźć w publikacji NIST SP 800-124 w wersji 2 (roboczej), *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [13]. Dodatkowo, w dokumencie NIAP *Protection Profile for Mobile Device Management* w wersji 4.0 [23] opisano ważne funkcje i wymagania bezpieczeństwa, których należy oczekiwać od systemów EMM.

3.6.1.3. WIRTUALNA SIEĆ PRYWATNA

Brama VPN zwiększa bezpieczeństwo zdalnych połączeń z autoryzowanych urządzeń mobilnych do wewnętrznej sieci organizacji. VPN to sieć wirtualna, zbudowana na bazie istniejących sieci fizycznych, która może zapewniać bezpieczny mechanizm komunikacji dla danych i informacji kontrolnych przesyłanych między sieciami. Sieci VPN są najczęściej używane do ochrony komunikacji przesyłanej przez sieci publiczne, takie jak Internet. Sieć VPN może zapewnić kilka rodzajów ochrony danych, w tym poufność, integralność, uwierzytelnianie pochodzenia danych, ochronę przed odtwarzaniem i kontrolę dostępu, które pomagają zmniejszyć ryzyko związane z ich przesyłaniem między komponentami sieci.

Połączenia VPN zapewniają dodatkową warstwę szyfrowania komunikacji między urządzeniami zdalnymi a siecią wewnętrzną, a bramy VPN mogą wymuszać decyzje dotyczące kontroli dostępu, określając, które urządzenia lub aplikacje mogą się z nimi łączyć. Integracja z innymi mechanizmami bezpieczeństwa umożliwia bramie VPN oparcie decyzji dotyczących kontroli dostępu na większej liczbie czynników ryzyka, niż może ona określić samodzielnie. Może to na przykład obejmować poziom zgodności urządzenia z zasadami bezpieczeństwa mobilnego lub listę zainstalowanych aplikacji,

które nie są dozwolone przez organizację, zgodnie z raportami zintegrowanego systemu EMM.

Publikacja NIAP *Extended Package for VPN Gateways* [24],w połączeniu z międzynarodowym i wspólnie opracowanym dokumentem *Protection Profile for Network Devices* [25], opisuje istotne możliwości i wymagania dotyczące bezpieczeństwa, których należy oczekiwać od bram VPN.

3.6.1.4. USŁUGA WERYFIKACJI APLIKACJI MOBILNYCH

Usługi weryfikacji aplikacji mobilnych wykorzystują różne statyczne, dynamiczne i behawioralne techniki do ustalania, czy aplikacja wykazuje jakiekolwiek działania stanowiące zagrożenie dla bezpieczeństwa lub prywatności. Ryzyko może dotyczyć właściciela lub użytkownika urządzenia, stron posiadających dane na urządzeniu lub systemów zewnętrznych, z którymi łączy się aplikacja. Zestaw wykrytych działań jest często agregowany w celu wygenerowania pojedynczego wyniku, będącego szacunkową wartością poziomu ryzyka (lub odwrotnie, zaufania) przypisanego do aplikacji. Klienci mogą często zmieniać wartości związane z danymi działaniami (np. kluczami kryptograficznymi w kodzie aplikacji), aby dostosować wynik do swojej unikalnej sytuacji związanej z ryzykiem. Wyniki te mogą być dalej agregowane w celu uzyskania wartości, która będzie odzwierciedlała ogólny poziom ryzyka lub zaufania związanego z zestawem aplikacji aktualnie zainstalowanych na danym urządzeniu.

Aplikacje mobilne, zarówno złośliwe, jak i niegroźne, mogą mieć znaczący negatywny wpływ zarówno na bezpieczeństwo, jak i prywatność użytkowników. Złośliwa aplikacja może zawierać kod mający na celu wykorzystanie podatności dowolnego komponentu sprzętowego, oprogramowania zwykłego i układowego urządzenia. Alternatywnie lub w połączeniu z kodem wykorzystującym luki w zabezpieczeniach, złośliwa aplikacja może niewłaściwie wykorzystywać wszelkie dane urządzenia, dane osobowe lub behawioralne, do których uzyskała bezpośredni lub dorozumiany dostęp, takie jak kontakty, dane schowka lub usługi lokalizacyjne. Niegroźne aplikacje mogą zawierać luki lub podatności, które złośliwe aplikacje mogą wykorzystać do uzyskania

nieautoryzowanego dostępu do ich danych lub funkcji. Co więcej, nieszkodliwe aplikacje mogą stanowić zagrożenie dla prywatności użytkownika, gromadząc więcej informacji niż jest to konieczne, aby zapewnić pożądane przez nie funkcje.

Chociaż nie jest to kwestia specyficzna dla aplikacji, niektóre usługi mogą uwzględniać w swojej analizie zagrożenia związane z urządzeniami (np. brak szyfrowania dysku lub podatną na ataki wersję systemu operacyjnego), aby zapewnić bardziej kompleksową ocenę ryzyka lub zaufania związanego z urządzeniem podczas korzystania z aplikacji lub usługi.

Organizacja NIAP nie opracowała profilu ochrony dla usług weryfikacji aplikacji. Jednak w dokumencie NIAP *Protection Profile for Application Software* [26] opisano wymogi bezpieczeństwa, których spełnienia należy oczekiwać od aplikacji mobilnych. Wielu dostawców usług weryfikacji aplikacji mobilnych zapewnia możliwości automatyzacji oceny aplikacji pod kątem wymogów NIAP.

3.6.1.5. OCHRONA PRZED ZAGROŻENIAMI MOBILNYMI

Ochrona przed zagrożeniami mobilnymi (*ang. Mobile Threat Defense – MTD*) ma zazwyczaj formę aplikacji instalowanej na urządzeniu, która zapewnia najszerszy i najbardziej aktualny dostęp do informacji o tym, jaka aktywność ma miejsce. W idealnej sytuacji rozwiązanie MTD jest w stanie wykryć niepożądaną aktywność i odpowiednio poinformować użytkownika, aby mógł on podjąć działania w celu zapobieżenia lub ograniczenia szkód, jakie może wyrządzić atakujący. Ponadto rozwiązanie MTD może być zintegrowane z rozwiązaniem EMM, aby wykorzystać jego możliwości na urządzeniu, takie jak blokowanie uruchomienia złośliwej aplikacji, dopóki użytkownik nie będzie mógł jej usunąć.

Produkty MTD analizują zazwyczaj ataki oparte na urządzeniach, aplikacjach i sieci. Zagrożenia związane z urządzeniami obejmują nieaktualne wersje systemu operacyjnego i niebezpieczne ustawienia konfiguracji. Zagrożenia związane z aplikacjami obejmują kwestie omówione powyżej w kontekście usług do weryfikacji aplikacji mobilnych, choć czasami nie mają one tak dużego zakresu, jak w przypadku

takich usług. Ataki sieciowe wiążą się z korzystaniem z niezaszyfrowanych lub publicznych sieci Wi-Fi oraz z aktywnymi próbami przechwytywania i odszyfrowywania ruchu sieciowego.

3.6.1.6. ANALIZA ZAGROŻEŃ MOBILNYCH

W tym przewodniku opisujemy analizę zagrożeń mobilnych jako przydatne informacje, które administratorzy urządzeń mobilnych mogą wykorzystać do wprowadzenia zmian w konfiguracji zabezpieczeń w celu poprawy poziomu bezpieczeństwa w odniesieniu do najnowszych rozwiązań. Dane takie obejmują złośliwe adresy URL, adresy IP, nazwy domen i nazwy aplikacji lub identyfikatory pakietów, a także sygnatury złośliwego oprogramowania lub podatności w aplikacjach, urządzeniach mobilnych, usługach platformy urządzeń lub mobilnych produktach zabezpieczających. Lista ta nie jest wyczerpująca, ponieważ wszelkie najnowsze informacje, które mogą stanowić podstawę do wprowadzenia szybkich zmian lepiej zabezpieczających wdrożenia mobilne przedsiębiorstwa przed nowymi lub nowo udoskonalonymi zagrożeniami, odnoszą się w równym stopniu do tego terminu. Takie możliwości można znaleźć w różnych innych rodzajach technologii, takich jak MTD i inne narzędzia do analizy sieci.

3.6.1.7. MOŻLIWOŚCI MOBILNEGO SYSTEMU OPERACYJNEGO

Możliwości mobilnego systemu operacyjnego są dostępne bez użycia dodatkowych funkcji bezpieczeństwa. Stanowią one część podstawowych funkcji urządzenia mobilnego. W urządzeniach mobilnych, w szczególności w telefonach komórkowych, dostępne są funkcje mobilnego systemu operacyjnego wymienione poniżej.

3.6.1.7.1. BEZPIECZNY ROZRUCH

Bezpieczny rozruch to ogólny termin odnoszący się do architektury systemu mającej na celu wykrywanie wszelkich nieautoryzowanych modyfikacji procesu rozruchu i zapobieganie im. System, który pomyślnie ukończy proces bezpiecznego rozruchu, wczytał informacje o sekwencji rozruchowej do zaufanego systemu operacyjnego. Powszechnym mechanizmem jest to, że pierwszy wykonywany program (moduł ładujący rozruch) jest niezmienny (przechowywany w pamięci tylko do odczytu lub

zaimplementowany wyłącznie sprzętowo). Co więcej, integralność zmiennego kodu jest kryptograficznie weryfikowana przed wykonaniem przez niezmienny lub zweryfikowany kod. Proces ten tworzy łańcuch zaufania, który można prześledzić wstecz do niezmiennego, domyślnie zaufanego kodu. Wykorzystanie zintegrowanego modułu TEE jako części bezpiecznego procesu rozruchu jest lepsze niż implementacja, w której zastosowano wyłącznie oprogramowanie [27].

3.6.1.7.2. ZAŚWIADCZANIE URZĄDZEŃ

Jest to rozszerzenie procesu bezpiecznego rozruchu dotyczące systemu operacyjnego (lub – częściej – zintegrowanego modułu TEE) zapewniające kryptograficznie weryfikowalny dowód, że ma on znaną i zaufaną tożsamość i jest w stanie godnym zaufania, co oznacza, że całe oprogramowanie działające na urządzeniu jest wolne od nieautoryzowanych modyfikacji.

Zaświadczanie urządzenia wymaga wykonania operacji kryptograficznych przy użyciu niezmiennego klucza prywatnego, który może zostać zweryfikowany przez zaufaną stronę trzecią, którą zazwyczaj jest producent oryginalnego modułu TEE (np. Qualcomm lub Samsung) lub dostawca platformy urządzenia (np. Google, Apple lub Microsoft). Dowód posiadania ważnego klucza stanowi o integralności pierwszego ogniwa w łańcuchu zaufania i chroni integralność wszystkich innych danych wykorzystywanych w procesie zaświadczania. Są to między innymi unikalne identyfikatory urządzeń, metadane i wyniki kontroli integralności modyfikowalnego oprogramowania oraz ewentualnie wskaźniki z samego procesu rozruchu lub zaświadczania [27].

3.6.1.7.3. ZARZĄDZANIE URZĄDZENIEM I INTERFEJS API MDM

Mobilne systemy operacyjne i zintegrowane z platformą oprogramowanie układowe (np. Samsung Knox) zapewniają szereg wbudowanych funkcji bezpieczeństwa, które są zazwyczaj domyślnie aktywne. Przykłady obejmują szyfrowanie na poziomie dysku i plików, weryfikację podpisów cyfrowych dla zainstalowanego oprogramowania i aktualizacji, kod odblokowujący urządzenie, zdalną blokadę urządzenia i automatyczne wymazywanie pamięci urządzenia po serii nieudanych prób jego

odblokowania. Niektóre z tych funkcji mogą być bezpośrednio konfigurowane przez użytkownika za pośrednictwem wbudowanej aplikacji lub usługi świadczonej przez dostawcę platformy urządzenia (np. Google, Apple lub Microsoft).

Ponadto interfejs API mobilnych systemów operacyjnych jest dostępny dla produktów MDM, dzięki czemu organizacja zarządzająca urządzeniem może mieć większą kontrolę nad tymi i wieloma innymi ustawieniami, które mogą nie być bezpośrednio dostępne dla użytkownika urządzenia. Interfejsy API do zarządzania umożliwiają przedsiębiorstwom korzystającym ze zintegrowanych produktów EMM lub MDM skuteczniejsze i wydajniejsze zarządzanie urządzeniami niż w przypadku korzystania wyłącznie z wbudowanej aplikacji.

4. ARCHITEKTURA

W tym punkcie czytelnik zapozna się z kwestiami dotyczącymi przykładowego rozwiązania, takimi jak:

- opis architektury
- mapa danych architektury bezpieczeństwa przedsiębiorstwa
- mapa środków bezpieczeństwa.

To przykładowe rozwiązanie składa się z sześciu technologii bezpieczeństwa mobilnego opisanych w punkcie 3.6: zaufanego środowiska wykonawczego, zarządzania mobilnością przedsiębiorstwa, wirtualnej sieci prywatnej, usługi weryfikacji aplikacji mobilnych, ochrony przed zagrożeniami mobilnymi i analizy zagrożeń mobilnych. W tabeli 4-1 wymieniono dostępne na rynku produkty wykorzystane w tym przykładowym rozwiązaniu oraz zestawiono je z sześcioma technologiami bezpieczeństwa mobilnego.

Tabela 4-1 Wykorzystane produkty dostępne na rynku

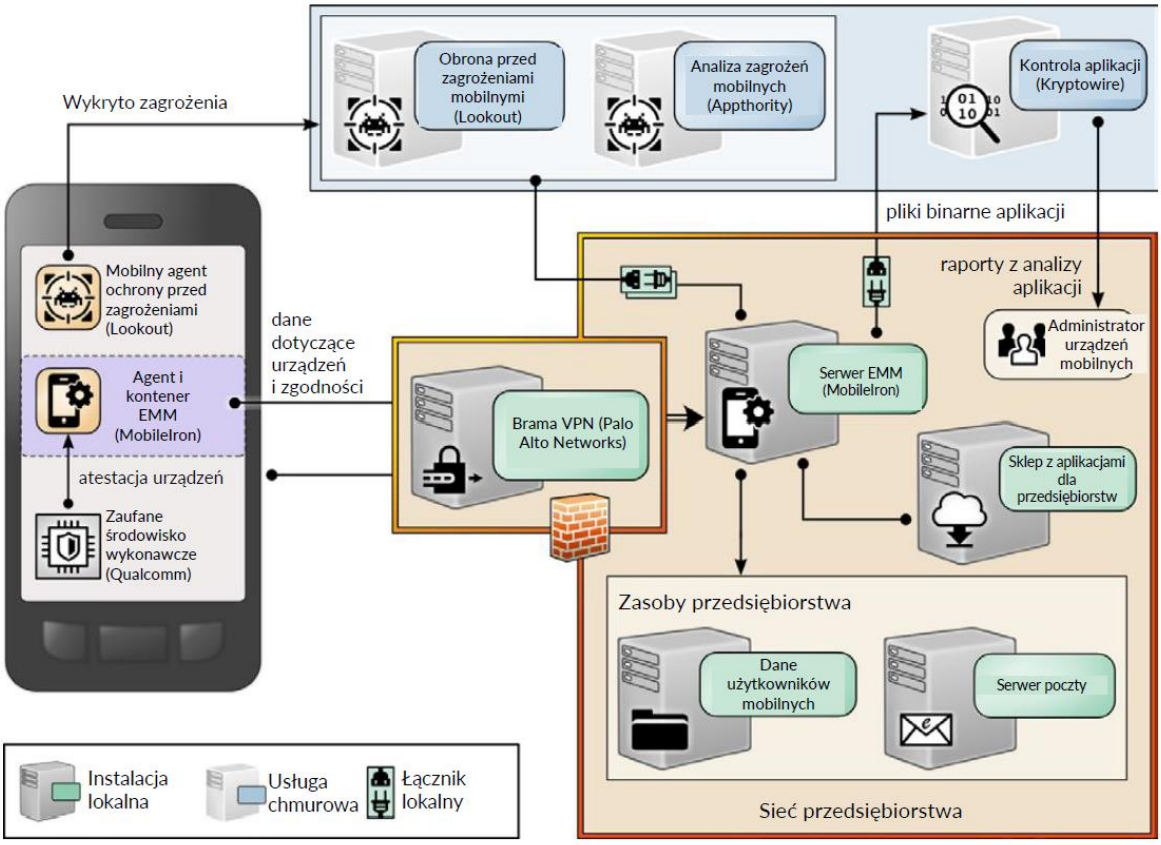
Produkt dostępny na rynku	Technologia bezpieczeństwa mobilnego
Appthority Cloud Service	Analiza zagrożeń mobilnych
Kryptowire Cloud Service	Usługa weryfikacji aplikacji mobilnych
Lookout Cloud Service/Lookout Agent w wersji 5.10.0.142 (iOS), 5.9.0.420 (Android)	Ochrona przed zagrożeniami mobilnymi
MobileIron Core w wersji 9.7.0.1, MobileIron Agent w wersji 11.0.1A (iOS), 10.2.1.1.3R (Android)	Zarządzanie mobilnością w przedsiębiorstwie
Palo Alto Networks, PA-220 w wersji 8.1.1	Wirtualna sieć prywatna
Qualcomm (wersja zależy od urządzenia mobilnego)	Zaufane środowisko wykonawcze

Komponenty te są dodatkowo zintegrowane z szerszymi lokalnymi mechanizmami bezpieczeństwa i bramą VPN, jak pokazano na rysunku 4-1. Takie zintegrowane rozwiązanie zapewnia szeroki wachlarz możliwości w zakresie bezpiecznego udostępniania urządzeń i zarządzania nimi, ochrony przed naruszeniem bezpieczeństwa urządzeń i wykrywania takich naruszeń, a także umożliwia

zapewnienie zwiększonego bezpieczeństwa dostępu do zasobów przedsiębiorstwa wyłącznie autoryzowanym użytkownikom i urządzeniom mobilnym.

Organizacje rozważające korzystanie z lokalnej technologii EMM powinny mieć świadomość, że będą odpowiedzialne za instalowanie i konfigurowanie jej lokalnych instancji. Obejmuje to bezpośrednie opłacenie przez organizację licencji na oprogramowanie dla wszelkich platform lub komponentów bazowych. Na rynku mogą być dostępne gotowe obrazy oprogramowania i kontenery, które mogą ułatwić instalowanie i konfigurowanie. Jako najlepszą praktykę zaleca się, aby w przypadku korzystania z gotowych kontenerów i obrazów sprawdzić je pod kątem typowych podatności oprogramowania.

Zaletą lokalnych rozwiązań do zarządzania urządzeniami mobilnymi jest to, że dane przedsiębiorstwa znajdują się w obrębie organizacji. Urządzenia, które mają odpowiednie uprawnienia, mogą nadal wysyłać i odbierać z rozwiązania dla urządzeń mobilnych informacje, do których otrzymywania są upoważnione. Zainteresowane organizacje mogą monitorować przepływ danych z rozwiązania EMM do innych urządzeń. Zainteresowane organizacje mogą monitorować przepływ danych z rozwiązania EMM do innych urządzeń.



Rysunek 4-1 Architektura przykładowego rozwiązania

4.1. OPIS ARCHITEKTURY

NCCoE we współpracy z ekspertami branżowymi opracowało otwartą, opartą na standardach, dostępną na rynku architekturę, która przeciwdziała zagrożeniom zidentyfikowanym podczas procesu szacowania ryzyka w punkcie 3.4.

Tam, gdzie to możliwe, w architekturze wykorzystano komponenty znajdujące się na liście zgodnych produktów NIAP [28],co oznacza, że produkt został pomyślnie oceniony pod kątem zatwierdzonego przez NIAP profilu ochrony [26]. NIAP współpracuje z szeroko pojętą społecznością, w tym z partnerami branżowymi, rządowymi i międzynarodowymi, aby publikować specyficzne dla technologii wymagania i testy bezpieczeństwa w formie profili ochrony. Wymagania i testy zawarte w tych profilach ochrony mają na celu zapewnienie, że oceniane produkty przeciwdziałają zidentyfikowanym zagrożeniom dla bezpieczeństwa.

Architektura przykładowego rozwiązania obsługuje pożądane funkcje bezpieczeństwa dzięki następującym integracjom.

4.1.1. INTEGRACJA W PRZEDSIĘBIORSTWIE

W przykładowym rozwiązaniu rozszerzono centralne zarządzanie tożsamością i dostępem na urządzenia mobilne poprzez integrację produktów MobileIron Core i Palo Alto Networks GlobalProtect z Microsoft Active Directory Domain Services (ADDS). Integralność identyfikacji i uwierzytelniania przez urządzenia mobilne w przedsiębiorstwie jest dodatkowo zwiększona dzięki wykorzystaniu certyfikatów urządzeń wydawanych przez lokalne usługi Microsoft Active Directory Certificate Service (ADCS).

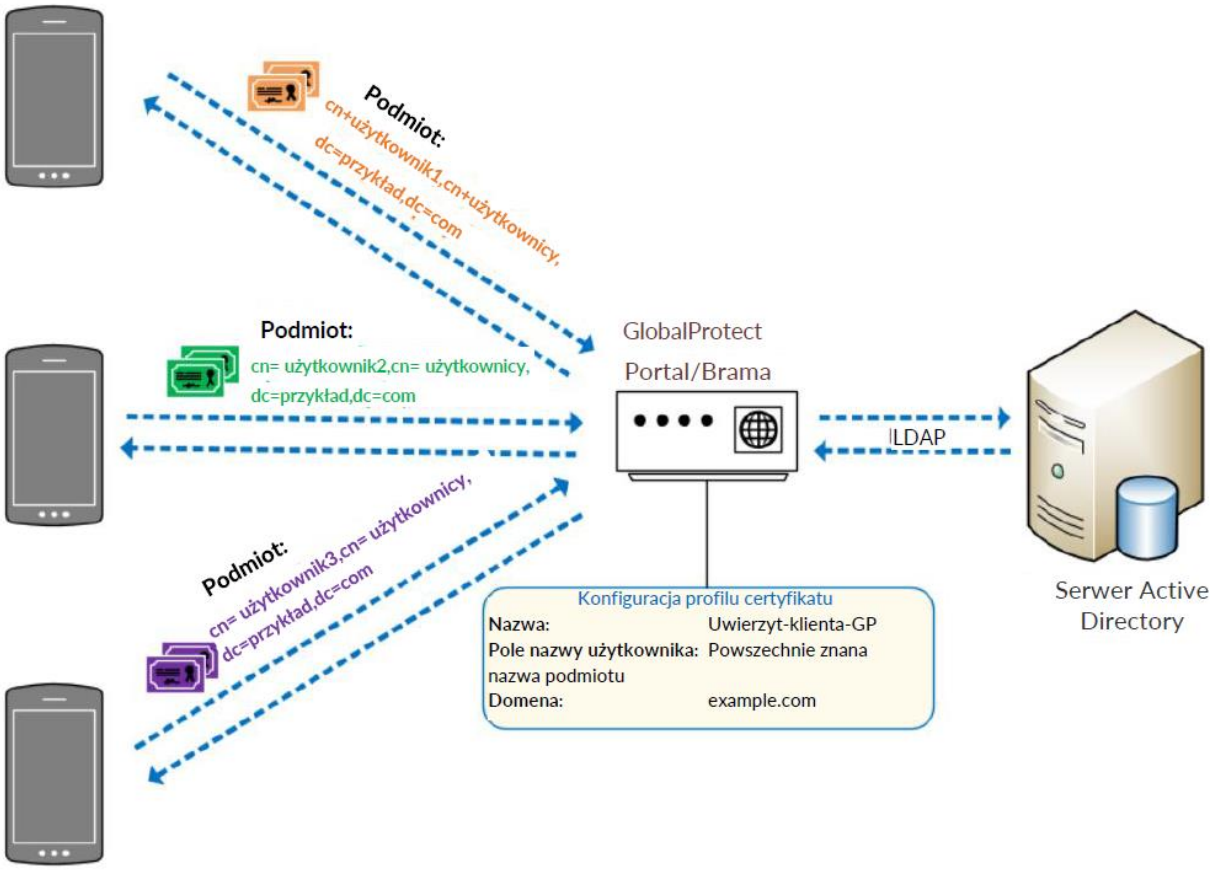
Dzięki integracji z AD, MobileIron Core umożliwia administratorom autoryzowanie wybranych grup użytkowników do rejestracji urządzeń mobilnych, ograniczając dostęp mobilny tylko do tych użytkowników, którzy go potrzebują. Ponadto różne zasady bezpieczeństwa, konfiguracje urządzeń i autoryzowane aplikacje mogą być wdrażane w różnych grupach AD, umożliwiając administratorom centralne zarządzanie różnymi przypadkami użycia urządzeń mobilnych. MobileIron Core wysyła zapytania do AD przy użyciu protokołu LDAP (*ang. lightweight directory access protocol*).

Dzięki integracji z ADCS, MobileIron Core automatycznie konfiguruje urządzenia, aby uzyskiwały lokalnie zarządzane certyfikaty urządzeń za pomocą protokołu SCEP (*ang. Simple Certificate Enrollment Protocol*). W naszym przykładowym rozwiązaniu ograniczono możliwość zdalnego wykorzystania podatności protokołu SCEP, ograniczając rejestrację certyfikatów do urządzeń mobilnych podłączonych do dedykowanej sieci Wi-Fi zarządzanej przez przedsiębiorstwo, która umożliwia urządzeniom dostęp wyłącznie do MobileIron Core i serwera NDES (*ang. Network Device Enrollment Service*). Co więcej, w przykładowym rozwiązaniu zastosowano dynamiczny schemat SCEP, w którym MobileIron Core zapewnia zarejestrowanemu urządzeniu mobilnemu jednorazowe hasło do uwzględnienia w żądaniu SCEP, uniemożliwiając w ten sposób nieznanym i niezaufanym urządzeniom, które uzyskują nieautoryzowany dostęp do dedykowanej sieci Wi-Fi, uzyskanie certyfikatu zaufanego urządzenia.

W konfiguracji rejestracji certyfikatu dla przykładowego rozwiązania w polu alternatywnej nazwy podmiotu certyfikatu urządzenia znajduje się główna nazwa użytkownika (*ang. User Principal Name – UPN*) użytkownika mobilnego, której brama VPN Palo Alto Networks GlobalProtect używa do sprawdzania poprawności łańcucha i wymuszania kontroli dostępu dla unikalnej kombinacji użytkownika mobilnego i urządzenia.

Urządzenia zarejestrowane w systemie MobileIron Core wykorzystują również pośrednio certyfikat urządzenia w celu zwiększenia bezpieczeństwa zdalnych połączeń z przedsiębiorstwem na dwa sposoby. Po pierwsze, komunikacja z systemem MobileIron Core (który musi być dostępny z Internetu w strefie zdemilitaryzowanej) jest zabezpieczona przy użyciu dwukierunkowego protokołu TLS (*ang. Transport Layer Security*). Zabezpiecza to system MobileIron Core przed nawiązywaniem bezpiecznych połączeń z niezaufanymi urządzeniami mobilnymi. Po drugie, certyfikat urządzenia jest wykorzystywany w konfiguracji sieci GlobalProtect VPN, co ogranicza dostęp do sieci VPN tylko do zaufanych urządzeń. Ponadto aplikacja GlobalProtect wykorzystuje UPN użytkownika urządzenia do przyznawania odpowiedniego dostępu do zasobów przedsiębiorstwa poprzez integrację z usługą ADDS.

Jak pokazano na rysunku 4-2 [29], urządzenia przedstawiają certyfikaty usługom uwierzytelniania VPN i EMM po pomyślnym wydaniu certyfikatów. Sieć VPN aplikacji GlobalProtect uwierzytelnia użytkownika urządzenia. Po pomyślnym uwierzytelnieniu aplikacja GlobalProtect wyświetla komunikat z prośbą o uwierzytelnienie użytkownika przy użyciu drugiego czynnika – hasła do domeny Active Directory. Po jego zweryfikowaniu aplikacja GlobalProtect ustanawia tunel z bramą i otrzymuje adres IP z puli IP w konfiguracji tunelu bramy.



Rysunek 4-2 Architektura bramy przykładowego rozwiązania

4.1.2. INTEGRACJA KOMPONENTÓW MOBILNYCH

W tym punkcie opisano, w jaki sposób różne komponenty technologii mobilnej są ze sobą zintegrowane. Większość tych komponentów jest zintegrowana z systemem EMM, MobileIron. MobileIron obsługuje integrację usług w chmurze dostawców zewnętrznych za pośrednictwem zdefiniowanego interfejsu API. MobileIron Core uwierzytelnia systemy zewnętrzne za pomocą podstawowego uwierzytelniania, więc protokół TLS chroni poufność poświadczeń konta API i odpowiedzi MobileIron na wywołania Representational State Transfer klientów. Konta klientów API MobileIron dla Kryptowire, Lookout Mobile Endpoint Security i Appthority Mobile Threat Protection (MTP) mają przypisane role administracyjne, które zapewniają minimalny zestaw uprawnień niezbędnych do osiągnięcia integracji [30], [31].

4.1.2.1. APPTHORITY – MOBILELRON

Usługa reputacji aplikacji Appthority zapewnia integrację z systemami MobileIron Core poprzez wdrożenie oprogramowania łączącego dostarczanego przez Appthority. Łącznik zapewnia kod, który obsługuje interfejsy API udostępniane przez system MobileIron Core i usługę w chmurze Appthority. w ramach tej integracji w systemie MobileIron Core utworzono użytkownika API i przypisano mu określone role konieczne do skutecznego działania usługi weryfikacji aplikacji.

Automatyczna synchronizacja między usługą Appthority a systemem MobileIron Core może odbywać się na podstawie konfiguracji. w szczególności między dwoma systemami synchronizowane są dane spisu aplikacji i urządzeń. w tej integracji synchronizacja odbywa się co godzinę, ale wartość ta powinna być dostosowana do potrzeb organizacji.

W przykładowym rozwiązaniu podstawową korzyścią z integracji jest egzekwowanie zgodności i eskalacja działań naprawczych. Na początkowym etapie procesu z systemu MobileIron Core pobierany jest spis aplikacji, a każdej z nich przypisywany jest wynik pomiaru zagrożenia. Jeśli aplikacja zostanie zainstalowana na urządzeniu, które nie jest zgodne ze skonfigurowaną polityką, Appthority MTP komunikuje się z systemem MobileIron Core w celu zidentyfikowania tych urządzeń, co uruchamia akcje egzekwowania zgodności MobileIron.

4.1.2.2. LOOKOUT – MOBILELRON

Usługa ochrony przed zagrożeniami mobilnymi Lookout umożliwia integrację z systemami MobileIron Core poprzez wdrożenie oprogramowania łączącego dostarczonego przez Lookout. Łącznik zapewnia kod, który obsługuje interfejsy API udostępniane przez system MobileIron Core i usługę w chmurze Lookout. Integracja ta umożliwia usłudze Lookout pobieranie szczegółowych informacji o urządzeniach, a także spisu aplikacji, a w razie potrzeby nadawanie etykiet urządzeniom.

Po przeprowadzeniu analizy usługa Lookout wykorzystuje interfejs API do nadawania urządzeniom określonych etykiet w celu ich kategoryzacji w oparciu o poziom ryzyka,

który jest obliczany na podstawie istotności problemów wykrytych na urządzeniu. System MobileIron może następnie automatycznie reagować na zastosowanie określonych etykiet w oparciu o wbudowane akcje zgodności. Umożliwia to administratorom dokładne skonfigurowanie sposobu, w jaki MobileIron będzie reagować na urządzenia należące do następujących kategorii:

- Pending (W toku) – nie aktywowano jeszcze usługi Lookout
- Secured (Zabezpieczone) – usługa Lookout aktywna
- Threats Present (Obecne zagrożenia) – usługa Lookout wykryła zagrożenia
- Deactivated (Dezaktywowano) – usługa Lookout została dezaktywowana
- Low Risk (Niskie ryzyko) – urządzenia z niską oceną ryzyka w usłudze Lookout
- Moderate Risk (Umiarkowane ryzyko) – urządzenia z umiarkowaną oceną ryzyka w usłudze Lookout
- High Risk (Wysokie ryzyko) – urządzenia z wysoką oceną ryzyka w usłudze Lookout

4.1.2.3. KRYPTOWIRE – MOBILELRON

Usługa Kryptowire uzyskuje szczegółowe informacje o urządzeniu, takie jak jego platforma, wersja systemu operacyjnego i uniwersalne unikalne identyfikatory przypisane do każdego urządzenia zarejestrowanego przez system MobileIron Core, aby umożliwić jednoznaczną identyfikację konkretnego urządzenia w różnych systemach. Kryptowire uzyskuje spis aplikacji ze wszystkich urządzeń zarejestrowanych w systemie MobileIron.

Kryptowire przeprowadza statyczną, dynamiczną i behawioralną analizę kodu binarnego aplikacji mobilnych pod kątem standardów rządowych (NIAP) i branżowych (*ang. Open Web Application Security Project – OWASP*) [32]. Kryptowire zapewnia szczegółową analizę bezpieczeństwa, dostarcza dowodów zgodności/niezgodności aż do poziomu wiersza kodu i podaje sumaryczną ważoną ocenę ryzyka dla każdej aplikacji.

Administratorzy aplikacji mobilnych mogą korzystać z takich szczegółowych raportów przy podejmowaniu decyzji o tym, które aplikacje są zaufane i zgodne z polityką bezpieczeństwa i prywatności przedsiębiorstwa, a które są ograniczone do użytku służbowego lub osobistego.

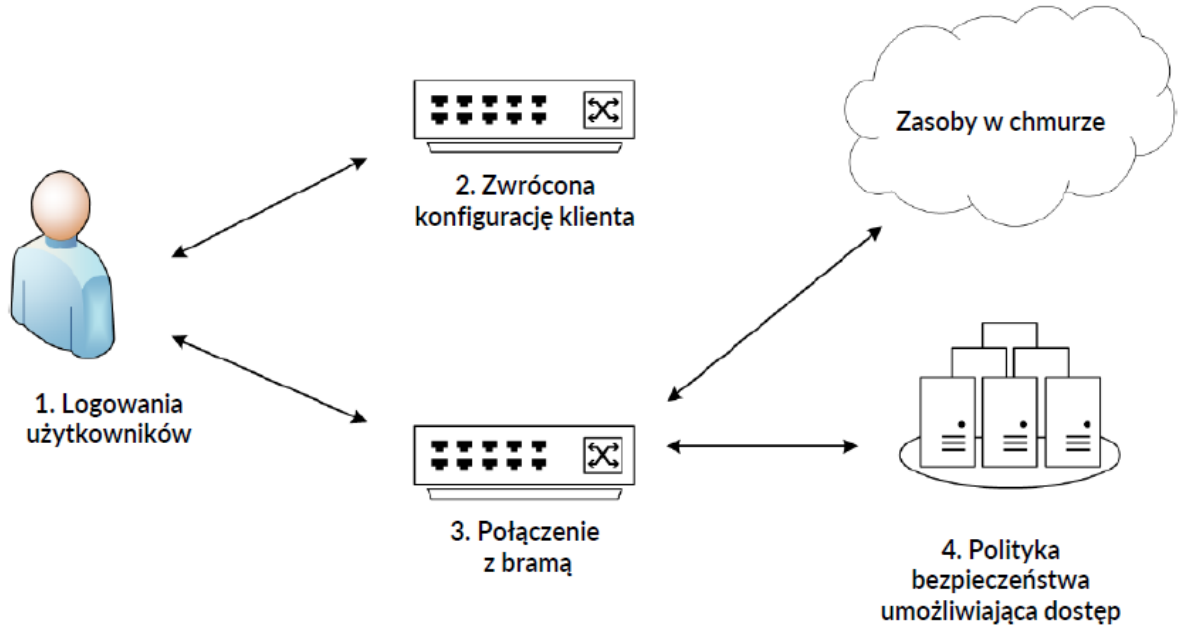
4.1.2.4. PALO ALTO NETWORKS – MOBILELRON

Usługa GlobalProtect VPN firmy Palo Alto Networks służy do zabezpieczania połączeń zdalnych z urządzeń mobilnych. System MobileIron Core obejmuje określone opcje konfiguracji dla klienta GlobalProtect – dostępnego dla systemów Android i iOS – które ułatwiają bezpieczne wdrażanie klientów VPN i włączanie dostępu VPN przy użyciu uwierzytelniania opartego na certyfikatach do bramy GlobalProtect. Szczegółowe informacje na temat procesu rejestracji certyfikatu znajdują się w punkcie 4.1.1

Architektura VPN zastosowana w tym przykładowym rozwiązaniu składa się z dwóch komponentów zapory nowej generacji Palo Alto Networks – portalu GlobalProtect i bramy GlobalProtect. Portal zapewnia funkcje zarządzania infrastrukturą VPN. Każdy punkt końcowy w sieci GlobalProtect otrzymuje informacje konfiguracyjne z portalu, w tym informacje o dostępnych bramach, a także wszelkie certyfikaty klienta, które mogą być wymagane do połączenia z bramami GlobalProtect.

Brama zapewnia egzekwowanie zasad bezpieczeństwa dla ruchu z aplikacji GlobalProtect. Jest ona skonfigurowana tak, aby zapewniać dostęp do określonych zasobów przedsiębiorstwa wyłącznie tym użytkownikom urządzeń mobilnych, którzy pomyślnie przejdą proces uwierzytelniania i autoryzacji.

Negocjacja konieczna do ustanowienia tunelu VPN pomiędzy punktem końcowym VPN/urządzeniem mobilnym a bramą VPN została przedstawiona na rysunku 4-3 [33]. Jak widać na rysunku, użytkownik loguje się do systemu (1), portal zwraca konfigurację klienta (2), agent automatycznie łączy się z bramą i ustanawia tunel VPN (3), a polityka bezpieczeństwa bramy umożliwia dostęp do aplikacji wewnętrznych i zewnętrznych (4).



Rysunek 4-3 Architektura VPN przykładowego rozwiązania

W naszym przykładowym rozwiązaniu zdecydowaliśmy się na wymuszenie konfiguracji, w której sieć VPN jest zawsze włączona. Konfiguracja ta powoduje, że zarejestrowane urządzenia nawiązują połączenie VPN z bramą GlobalProtect za każdym razem, gdy mają łączność z siecią – dzieje się to za pośrednictwem sieci komórkowej lub Wi-Fi, a połączenie jest ponawiane po ponownym uruchomieniu urządzenia. Taka konfiguracja zapewnia urządzeniom najwyższy stopień ochrony, ponieważ GlobalProtect można rozszerzyć o dodatkowe usługi Palo Alto Networks. W tym przykładowym rozwiązaniu zastosowano filtrowanie adresów URL, które blokuje urządzeniom mobilnym dostęp do zabronionych domen internetowych lub wszelkich domen, które Palo Alto Networks powiązało z próbami wykorzystywania podatności (np. kampaniami wyłudzania informacji, atakami typu *watering hole* czy *botnet command and control*). w publikacji NIST SP 800-46 w wersji 2, *Guide to Enterprise Telework, Remote Access, and BYOD Security* [34], opisano najczęstsze opcje sieci VPN stosowane w przypadku pracowników zdalnych.

4.1.2.4.1. ZGODNOŚĆ Z NORMĄ FIPS

Poufność i integralność wszelkich wrażliwych informacji przesyłanych przez Internet, sieci bezprzewodowe i inne niezaufane sieci powinna być chroniona za pomocą

kryptografii [34]. Agencje federalne są zobowiązane do stosowania algorytmów kryptograficznych zatwierdzonych przez NIST i zawartych w modułach zatwierdzonych w ramach federalnych standardów przetwarzania informacji (*ang. Federal Information Processing Standards – FIPS*), ale wdrożenie tych standardów jest również dostępne dla organizacji prywatnych i komercyjnych [35]. W przykładowym rozwiązaniu zastosowano te najlepsze praktyki w następujący sposób:

- W ramach usługi GlobalProtect VPN włączony jest tryb FIPS-CC, który wymaga protokołu TLS 1.1 (lub nowszego) i ogranicza użycie klucza publicznego do algorytmów zatwierdzonych w FIPS. W implementacji tego przykładowego rozwiązania wykorzystano najnowszą dostępną wersję TLS, przy czym najstarszą akceptowalną wersją jest TLS 1.2. Pełna lista funkcji bezpieczeństwa znajduje się na stronie dokumentacji Palo Alto Networks FIPSCC Security Functions [36].
- Jak opisano w punkcie 4.1.1, włączone są dynamiczne testy SCEP.

Aby dostosować nasze przykładowe rozwiązanie do wytycznych zawartych w publikacji NIST SP 800-52[6] w wersji 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* [37], w niniejszym przykładzie zaimplementowano następującą konfigurację:

- Portal i brama GlobalProtect ograniczają listę zestawów szyfrowania dostępnych dla aplikacji klienckiej za pomocą profilu usługi TLS. Zgodnie z zaleceniami zawartymi w publikacji NIST SP 800-52 ustawiona najstarsza możliwa wersja protokołu TLS to 1.2.
- Dla certyfikatów portalu GlobalProtect i serwera bramy używany jest 2048-bitowy moduł klucza RSA podpisany przy użyciu algorytmu sha256WithRSAEncryption.

4.1.2.5. INTEGRACJA ROZWIĄZANIA EMM Z SYSTEMAMI IOS I ANDROID

Zarówno urządzenia z systemem iOS, jak i Android można bezpośrednio zintegrować z rozwiązaniami EMM, zapewniając zarządzanie środkami bezpieczeństwa na poziomie przedsiębiorstwa w oparciu o odpowiednie zasady.

[6] Polskojęzyczna publikacja NSC 800-52.

Integracja z systemem iOS

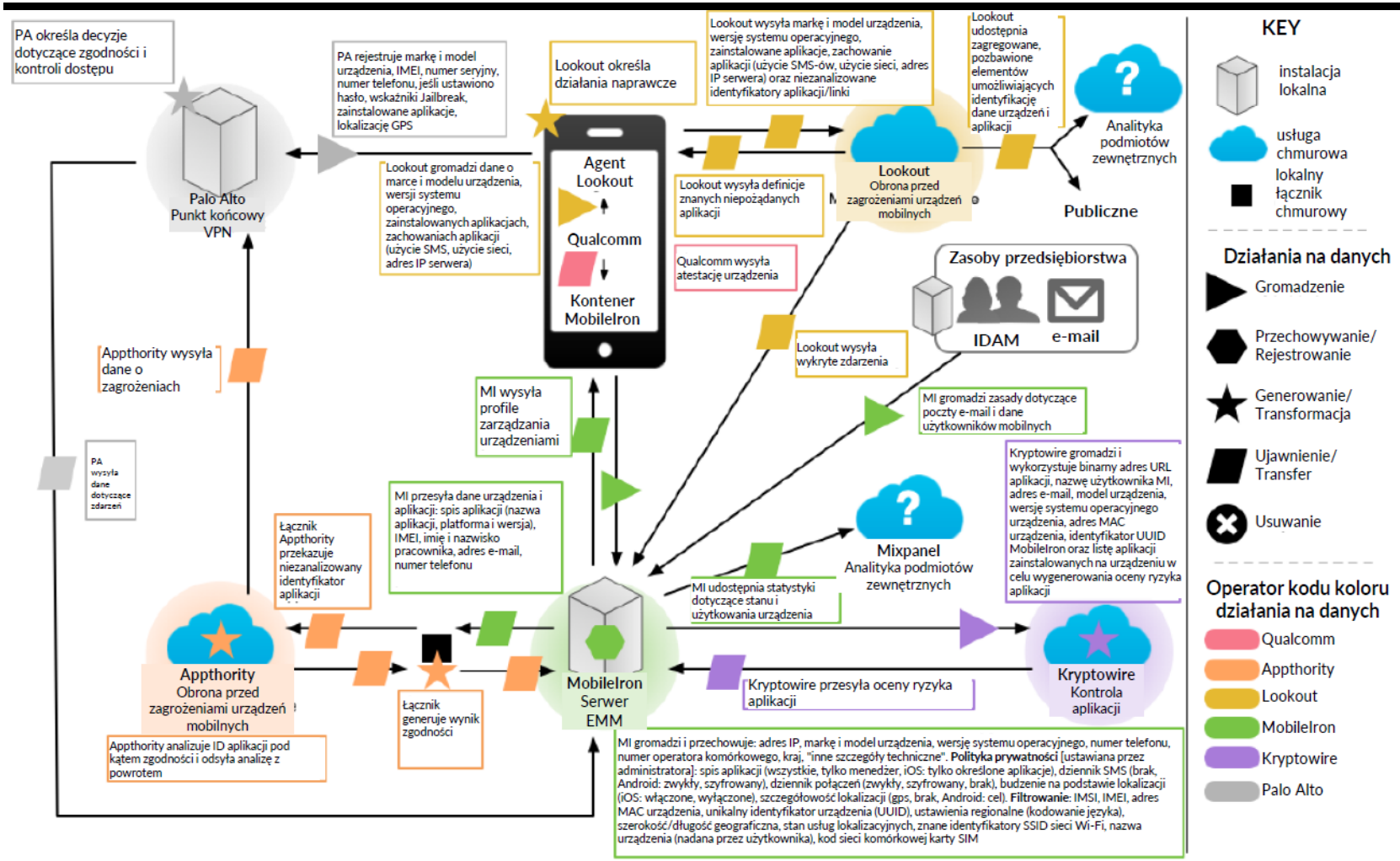
Urządzenia iOS są zarządzane za pośrednictwem profili konfiguracji. Profile konfiguracji mogą wymuszać stosowanie zasad bezpieczeństwa, takich jak korzystanie z sieci VPN, obsługa protokołu Kerberos w przedsiębiorstwie i dostęp do usług w chmurze. System iOS zawiera ponadto zestaw dodatkowych zabezpieczeń w tak zwanym trybie nadzorowanym, który jest stosowany na urządzeniach należących do firmy. Zazwyczaj w przypadku wdrażania urządzeń z systemem iOS na dużą skalę w trybie nadzorowanym organizacje decydują się na korzystanie z usługi Apple Business Manager (dawniej Device Enrollment Program) [38] ze względu na oszczędność pracy związanej z ręcznym konfigurowaniem każdego urządzenia. Jednak ponieważ liczba urządzeń w naszym projekcie referencyjnym jest niewielka, skonfigurowaliśmy tryb nadzorowany za pomocą narzędzia Apple Configurator 2 [39]. Opis zdolności do ochrony systemu iOS można znaleźć w dokumencie Apple Platform Security [40].

Integracja z systemem Android

Analogicznie, urządzenia z systemem Android są wyposażone w środki bezpieczeństwa, które system EMM może wykorzystać w ramach wdrożeń w przedsiębiorstwach. Program Android Enterprise firmy Google jest dostępny na urządzeniach z systemem Android w wersji 5.0 (Lollipop) lub nowszej. System EMM wdraża kontroler zasad [41] jako część swojego agenta na urządzeniu. Kontroluje on lokalne zasady dotyczące urządzeń i aplikacje systemowe na urządzeniach. Nowszy tryb wprowadzony w systemie Android 8.0 obsługuje w pełni zarządzane urządzenia z profilem służbowym, przeznaczone do wdrożeń COPE [42], [43], [44]. W tym scenariuszu urządzenie jest własnością firmy. Dostępne są funkcje bezpieczeństwa na poziomie urządzenia, takie jak czyszczenie jego pamięci i przywracanie domyślnych ustawień fabrycznych. Tworzony jest również profil służbowy, aby oddzielić aplikacje i dane firmowe od wszelkich danych osobistych. Scenariusz ten zapewnia właścicielowi urządzenia pewną elastyczność umożliwiając mu korzystanie z urządzenia do celów osobistych przy jednoczesnym zachowaniu bezpieczeństwa i jest wybranym sposobem wdrożenia w tym projekcie referencyjnym.

4.2. MAPA DANYCH PRYWATNOŚCI W ARCHITEKTURZE BEZPIECZEŃSTWA PRZEDSIĘBIORSTWA

Firma Orvilia przeprowadziła analizę prywatności, uwzględniając zarówno informacje zebrane podczas początkowych prac z wykorzystaniem metodologii PRAM, jak i zidentyfikowane technologie bezpieczeństwa mobilnego uwzględnione w zmienionej architekturze. Wyniki działań z wykorzystaniem PRAM, w tym przepływy danych między komponentami wraz z ich lokalizacją – lokalnie lub w chmurze – dały w rezultacie informacje zawarte na rysunku 4-4. Uwaga: Legenda do tego rysunku opisuje wszystkie typy działań związanych z danymi, ale to konkretne przykładowe rozwiązanie nie obejmuje usuwania danych z ćwiczenia mapowania danych osobowych. Dodatkowe informacje na temat działań z wykorzystaniem metodologii PRAM można znaleźć w załączniku G.



Rysunek 4-4 Mapa danych metodologii NIST szacowania ryzyka w odniesieniu do prywatności dla architektury bezpieczeństwa przedsiębiorstwa Orvilia.

Tłumaczenie

4.3. MAPA ŚRODKÓW BEZPIECZEŃSTWA

Wykorzystując uzyskane informacje o ryzyku jako dane wejściowe, określono charakterystykę bezpieczeństwa rozwiązania. Opracowano mapę środków bezpieczeństwa, w której zestawiono możliwości przykładowego rozwiązania z odpowiednimi podkategoriami z ram cyberbezpieczeństwa NIST w wersji 1.1 [5]; publikacji NIST SP 800-53 w wersji 4, *Security and Privacy Controls for Federal Information Systems and Organizations [11]*; Międzynarodowej Organizacji Normalizacyjnej (ISO), Międzynarodowej Komisji Elektrotechnicznej (IEC) 27001:2013, *Information technology-Security techniques-Information security management systems Requirements* [45]; zestawu środków bezpieczeństwa Center for Internet Security [46] w wersji 6; oraz publikacji NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [7].

W ramach mapy środków bezpieczeństwa określono mapowanie standardów cech bezpieczeństwa dla produktów, które zostały wykorzystane w przykładowym rozwiązaniu. Produkty mogą mieć dodatkowe funkcje, które nie zostały wykorzystane w tym przykładowym rozwiązaniu. Z tego powodu zaleca się, aby mapa ta nie była używana jako źródło informacji o wszystkich funkcjach bezpieczeństwa, które produkty te mogą obsługiwać. Mapa środków bezpieczeństwa znajduje się w tabeli I-1.

5. ANALIZA CHARAKTERYSTYKI BEZPIECZEŃSTWA

W niniejszym punkcie czytelnik zapozna się z następującymi zagadnieniami:

- założenia i ograniczenia,
- testowanie projektu,
- scenariusze i wnioski.

Celem analizy charakterystyki bezpieczeństwa jest zrozumienie, w jakim stopniu projekt spełnia swój cel — zademonstrowanie, w jaki sposób zwiększyć bezpieczeństwo urządzeń mobilnych w przedsiębiorstwie poprzez wdrożenie systemu EMM, MTD, MTI, weryfikacji aplikacji, bezpiecznego rozruchu/uwierzytelniania obrazu i usług VPN.

5.1. ZAŁOŻENIA I OGRANICZENIA ANALIZY

Analiza charakterystyki bezpieczeństwa ma następujące ograniczenia:

- Nie jest to ani kompleksowe badanie wszystkich elementów bezpieczeństwa, ani test typu Red Team.
- Nie może zidentyfikować wszystkich słabych punktów.
- Nie obejmuje infrastruktury laboratoryjnej. Zakłada się, że systemy te są zabezpieczone. Testowanie tych urządzeń ujawniłoby tylko słabości w implementacji, które nie byłyby istotne dla tych, którzy wdrażają taką architekturę referencyjną.

5.2. TESTOWANIE PROJEKTU

Testy funkcjonalne zostały wykorzystane do potwierdzenia możliwości przykładowego rozwiązania. Korzystając z działań testowych, demonstrujemy podatność Orvilii na zagrożenia przed wdrożeniem architektury opisanej w niniejszym przewodniku po praktykach. Następnie ponownie wykorzystujemy działania testowe po wdrożeniu architektury, aby wykazać, że odpowiednio przeciwdziała ona zagrożeniom.

5.2.1. ZDARZENIE POWODUJĄCE ZAGROŻENIE 1 (TE1) — NIEAUTORYZOWANY DOSTĘP DO POUFNYCH INFORMACJI ZA POŚREDNICTWEM ZŁOŚLIWEJ LUB NARUSZAJĄCEJ PRYWATNOŚĆ APLIKACJI

Podsumowanie: Testowany jest nieautoryzowany dostęp do wrażliwych informacji za pośrednictwem złośliwej lub naruszającej prywatność aplikacji. Przetestowaliśmy to zagrożenie, umieszczając na urządzeniach fałszywą wrażliwą listę kontaktów i wpisy kalendarza, a następnie próbując zainstalować i używać aplikacji z Apple App Store i Google Play Store [47] które uzyskiwały dostęp do tych danych i tworzyły ich kopie zapasowe. W idealnym przypadku architektura bezpieczeństwa przedsiębiorstwa wykryłaby lub uniemożliwiłaby korzystanie z tych aplikacji, albo zablokowałaby aplikacjom dostęp do listy kontaktów i wpisów kalendarza będących pod kontrolą przedsiębiorstwa.

Działanie testowe: Zainstalowanie aplikacji dla systemu iOS lub Android, która uzyskuje dostęp do kontaktów i wpisów kalendarza oraz tworzy ich kopie zapasowe w chmurze. Nie mamy powodu, aby podejrzewać, że te aplikacje są złośliwe. Jednak działanie polegające na uzyskiwaniu dostępu i tworzeniu kopii zapasowych danych kontrolowanych przez przedsiębiorstwo (kontakty i wpisy kalendarza) bez autoryzacji stanowi działanie, któremu powinna zapobiegać architektura bezpieczeństwa tego przykładowego rozwiązania.

Pożądany rezultat: Architektura bezpieczeństwa w przedsiębiorstwie powinna wykrywać obecność aplikacji i fakt, że uzyskują one dostęp do kontaktów i wpisów kalendarza. Architektura bezpieczeństwa powinna blokować instalację tych aplikacji, blokować ich uruchamianie lub wykrywać ich obecność i powodować inną odpowiednią reakcję, taką jak blokowanie dostępu urządzenia mobilnego do zasobów przedsiębiorstwa do czasu usunięcia aplikacji.

Alternatywnie, wbudowane mechanizmy urządzenia, takie jak funkcja do obsługi zarządzanych aplikacji firmy Apple i funkcja profilu służbowego Google Android, mogą być użyte do oddzielenia kontaktów i wpisów kalendarza powiązanych z firmowymi kontami e-mail, tak aby dostęp do nich miały tylko aplikacje firmowe (aplikacje

autoryzowane i zarządzane za pośrednictwem systemu EMM), a nie aplikacje instalowane ręcznie przez użytkownika. Użytkownik nie powinien mieć możliwości ręcznego udostępniania swojego firmowego konta e-mail. Konto powinno być udostępniane tylko za pośrednictwem systemu EMM, aby przedsiębiorstwo miało kontrolę nad firmową listą kontaktów i danymi kalendarza. Jednak w projekcie opisanym w niniejszym przewodniku po praktykach zdecydowaliśmy się na w pełni zarządzane urządzenia, nie dzieląc ich na osobne obszary firmowe i osobiste.

Zaobserwowany rezultat: Usługa Appthority wykryła obecność aplikacji, które mają dostęp do wrażliwych danych i zaktualizowała etykiety urządzeń w systemie MobileIron Core.

5.2.2. ZDARZENIE POWODUJĄCE ZAGROŻENIE 2 (TE-2) — KRADZIEŻ DANYCH UWIERZYTELNIAJĄCYCH ZA POŚREDNICTWEM KAMPANII WIADOMOŚCI SMS LUB E-MAIL SŁUŻĄCEJ DO WYŁUDZANIA INFORMACJI

Podsumowanie: Stworzono fikcyjny atak polegający na wyłudzaniu informacji, w którym przetestowano ochronę przed kradzieżą danych uwierzytelniających za pośrednictwem kampanii wiadomości SMS lub e-mail.

Działanie testowe:

- Utworzenie strony internetowej z formularzem podobnym do monitu z systemu przedsiębiorstwa o konieczności zalogowania się.
- Wysłanie adresu URL strony internetowej za pośrednictwem wiadomości SMS lub e-mail i podjęcie próby pozyskania i wykorzystania danych logowania do systemu przedsiębiorstwa.

Pożądany rezultat: Architektura bezpieczeństwa przedsiębiorstwa powinna uniemożliwiać użytkownikowi przeglądanie znanych złośliwych stron internetowych. Ponadto przedsiębiorstwo powinno korzystać z uwierzytelniania wieloskładnikowego lub metod uwierzytelniania odpornych na wyłudzanie informacji – takich jak te oparte na kryptografii klucza publicznego – tak aby złośliwy podmiot nie mógł przechwycić hasła lub przechwycenie hasła było niewystarczające do uzyskania dostępu do zasobów przedsiębiorstwa.

Zaobserwowany rezultat: w przykładowym rozwiązaniu wykorzystano zaporę sieciową nowej generacji Palo Alto Networks. Zapora obejmuje usługę filtrowania adresów URL PAN-DB, która automatycznie blokuje znane złośliwe adresy URL. Baza danych filtrowania jest regularnie aktualizowana, aby zapewnić użytkownikom ochronę przed złośliwymi adresami URL. Zapora nowej generacji zablokowała próbę odwiedzenia strony wyłudzającej informacje, ponieważ złośliwy adres URL był w bazie danych PAN-DB. Uniemożliwiło to użytkownikowi dostęp do strony wyłudzającej informacje.

5.2.3. ZDARZENIE POWODUJĄCE ZAGROŻENIE 3 — ZŁOŚLIWE APLIKACJE INSTALOWANE ZA POŚREDNICTWEM ADRESU URL W WIADOMOŚCIACH SMS LUB E-MAIL

Podsumowanie: Nieautoryzowane aplikacje, które nie są dostępne w oficjalnym sklepie Apple App Store lub Google Play Store, są instalowane za pośrednictwem łączy URL w wiadomościach SMS, e-mail lub witrynach internetowych innych firm.

Działanie testowe (Android):

- Wysłanie do użytkownika wiadomości e-mail zawierającej łącze do pliku o treści zachęcającej do kliknięcia go w celu zainstalowania aplikacji.
- Jeśli opcja ta nie została jeszcze włączona w ustawieniach zabezpieczeń urządzenia, należy spróbować aktywować przełącznik Unknown Sources (Nieznane źródła), aby zezwolić na instalowanie aplikacji ze źródeł innych niż Sklep Google Play.
- Korzystając z urządzenia, należy przeczytać otrzymaną wiadomość e-mail, kliknąć łącze i spróbować zainstalować aplikację F-Droid.
- Sprawdzić, czy aplikacja F-Droid została pomyślnie zainstalowana. Jeśli tak, należy ustalić, czy przedsiębiorstwo wykryło instalację nieautoryzowanej aplikacji i odpowiednio zareagowało.

Działanie testowe (iOS):

- Wysłanie do użytkownika wiadomości e-mail zawierającej łącze do aplikacji iOS dostępnej do zainstalowania ze strony internetowej, wraz z treścią zachęcającą go do kliknięcia łącza w celu jej zainstalowania.

- Korzystając z urządzenia, należy przeczytać otrzymaną wiadomość e-mail, kliknąć łącze i spróbować zainstalować aplikację.
- Korzystając z urządzenia, należy podjąć próbę udzielenia wyraźnego zaufania do certyfikatu podpisu dewelopera. Następnie spróbować uruchomić aplikację.
- Sprawdzić, czy aplikację da się uruchomić. Jeśli tak, należy ustalić, czy przedsiębiorstwo wykryło instalację nieautoryzowanej aplikacji i odpowiednio zareagowało.

Pożądany rezultat: Urządzenie nie zezwala użytkownikowi na zainstalowanie nieautoryzowanej aplikacji. Jeśli aplikacja zostanie w jakiś sposób zainstalowana, jej obecność powinna być wykryta i powinna nastąpić odpowiednia reakcja, taka jak zablokowanie dostępu urządzenia do zasobów przedsiębiorstwa do czasu usunięcia aplikacji.

Zaobserwowany rezultat: Na urządzeniach z systemem iOS usługa Lookout wykryła, że aplikacja została zainstalowana lokalnie i nadała urządzeniu odpowiednią etykietę. Następnie system MobileIron poddał urządzenie kwarantannie (odebrał mu dostęp do zasobów przedsiębiorstwa) do czasu wyeliminowania zagrożenia.

W przypadku urządzeń z systemem iOS, system MobileIron ma opcję konfiguracji, która uniemożliwiał użytkownikowi zaufanie certyfikatowi dewelopera.

W przypadku urządzeń z systemem Android, system MobileIron ma opcję konfiguracji, która uniemożliwia użytkownikowi włączenie instalowania aplikacji z nieznanych źródeł.

5.2.4. ZDARZENIE POWODUJĄCE ZAGROŻENIE 4 — UTRATA POUFNOŚCI I INTEGRALNOŚCI W WYNIKU WYKORZYSTANIA ZNANEJ PODATNOŚCI W SYSTEMIE OPERACYJNYM LUB OPROGRAMOWANIU UKŁADOWYM

Podsumowanie: Gdy złośliwe oprogramowanie z powodzeniem wykorzystuje lukę w zabezpieczeniach mobilnego systemu operacyjnego lub sterowników urządzenia, wprowadzony kod jest zazwyczaj wykonywany z podwyższonymi uprawnieniami, a następnie wydaje polecenia z poziomu użytkownika głównego lub jądra systemu operacyjnego.

Działanie testowe: Próba uzyskania dostępu do zasobów przedsiębiorstwa z urządzenia mobilnego o znanych lukach w zabezpieczeniach (np. ze starszą, niezaktualizowaną wersją systemu iOS lub Android).

Pożądany rezultat: Architektura bezpieczeństwa przedsiębiorstwa powinna wykryć obecność urządzeń z nieaktualną wersją systemu iOS lub Android o znanych podatnościach na ataki. Jeśli jest to uzasadnione ryzykiem, powinna istnieć możliwość zablokowania urządzeniom dostępu do zasobów przedsiębiorstwa do czasu zainstalowania aktualizacji systemu.

Zaobserwowany rezultat: Usługa Lookout wykryła, że na urządzeniach były zainstalowane nieaktualne wersje systemów operacyjnych. Informacja ta została przekazana do systemu MobileIron, który następnie automatycznie poddał urządzenia kwarantannie do czasu aktualizacji systemu operacyjnego.

5.2.5. ZDARZENIE POWODUJĄCE ZAGROŻENIE 5 — NARUSZENIE PRYWATNOŚCI POPRZEZ NIEWŁAŚCIWE WYKORZYSTANIE CZUJNIKÓW URZĄDZENIA

Podsumowanie: Dane dotyczące lokalizacji, z kamery lub mikrofonu, są gromadzone przez aplikację, która nie powinna mieć dostępu do takich danych.

Uwaga: Nie wszystkie aplikacje, które mają dostęp do danych lokalizacji, z kamery lub mikrofonu, są złośliwe. Jednakże, jeśli okaże się, że aplikacja gromadzi takie informacje, może być konieczna dodatkowa weryfikacja lub testy w celu określenia ich ewentualnego przeznaczenia, a następnie ustalenia, czy aplikacja jest złośliwa. **Działanie testowe:** Przesłanie aplikacji do usługi Kryptowire i zapoznanie się z raportem wyjściowym.

Pożądany rezultat: W raporcie wyjściowym stwierdzono wykorzystanie lokalizacji, danych z kamery lub mikrofonu przez aplikację.

Zaobserwowany rezultat: W raporcie usługi Kryptowire stwierdzono wykorzystanie przez aplikację czujnika lokalizacji, kamery lub mikrofonu. Administrator może następnie przeprowadzić dalsze testy aplikacji i w razie potrzeby oznaczyć ją jako zabronioną w systemie EMM.

5.2.6. ZDARZENIE POWODUJĄCE ZAGROŻENIE 6 — NARUSZENIE INTEGRALNOŚCI URZĄDZENIA LUB JEGO KOMUNIKACJI SIECIOWEJ POPRZEZ INSTALACJĘ ZŁOŚLIWEGO SYSTEMU EMM/MDM, SIECI, PROFILI VPN LUB CERTYFIKATÓW

Podsumowanie: Dochodzi do naruszenia integralności urządzenia lub jego komunikacji sieciowej poprzez instalację złośliwego systemu EMM/MDM, sieci, profili VPN lub certyfikatów na drodze ataku typu „*person-in-the-middle*".

Działanie testowe:

- Zainstalowanie aplikacji mitmproxy (https://mitmproxy.org/) na komputerze (my użyliśmy komputera Mac) podłączonym do tej samej sieci Wi-Fi, co urządzenia mobilne.
- Zainstalowanie certyfikatu CA mitmproxy (przechowywanego w lokalizacji ~/.mitmproxy/mitmproxy-ca-cert.cer na komputerze Mac) na testowanych urządzeniach mobilnych. Instrukcje dla systemów iOS i Android znajdują się poniżej.
- Skonfigurowanie komputera w sposób niezbędny do uruchomienia mitmproxy w trybie transparentnym, zgodnie z opisem na stronie https://docs.mitmproxy.org/stable/howto-transparent/.
- Aby zaprezentować zdolność złośliwego podmiotu do manipulowania ruchem sieciowym, pobraliśmy skrypt mitmproxy internet_in_mirror ze strony https://docs.mitmproxy.org/stable/addons-examples/#internet-in-mirror. Tworzy on lustrzane odbicie zawartości wszystkich stron internetowych.
- Należy uruchomić mitmproxy w trybie transparentnym, używając skryptu internet_in_mirror: mitmproxy-mode transparent-ssl-insecure-showhost-s internet_in_mirror.py
- Zamiast przeprowadzać inwazyjny atak, taki jak fałszowanie protokołu rozpoznawania adresów, ręcznie skonfigurowaliśmy ustawienia sieci Wi-Fi każdego urządzenia mobilnego zmieniając adres IP domyślnej bramy (czasami nazywanej routerem w ustawieniach sieci) na adres IP komputera, zamiast adresu

IP routera. Ta zmiana konfiguracji wymusiła przepływ całego ruchu sieciowego z każdego urządzenia przez komputer.

Działanie testowe (Android):

- Umieścić certyfikat CA mitmproxy jako załącznika w wiadomości e-mail.
- Otworzyć wiadomość e-mail na urządzeniu z systemem Android i kliknąć załącznik, aby dokonać próby instalacji certyfikatu CA.
- Zmodyfikować ustawienia sieci Wi-Fi urządzenia, ręcznie zmieniając adres IP domyślnej bramy na adres komputera z uruchomioną aplikacją mitmproxy.
- Przejść na stronę zabezpieczoną protokołem HTTPS (np. https://www.nccoe.nist.gov) i sprawdzić, czy zawartość została odwrócona, co świadczy o tym, że atak typu „person-in-the-middle" na połączenie zabezpieczone protokołem TLS zakończył się powodzeniem.

Działanie testowe (iOS):

- Użyć programu Apple Configurator 2 na komputerze Mac lub innego narzędzia, aby utworzyć profil konfiguracji systemu iOS zawierający certyfikat CA mitmproxy. Profil konfiguracji użyty w testach nosił nazwę Enterprise Access. Profil konfiguracji został podpisany przy użyciu klucza powiązanego z certyfikatem bezpłatnego konta programisty Apple. Podpis był opcjonalny (profile konfiguracji nie muszą być podpisywane).
- Wysłać profil konfiguracji jako załącznik do wiadomości e-mail.
- Otworzyć wiadomość e-mail i spróbować kliknąć załącznik, aby zainstalować profil konfiguracji. Spróbować postępować zgodnie z instrukcjami, aby dokończyć instalację profilu.
- Spróbować włączyć certyfikat CA w ustawieniach zaufania certyfikatów urządzenia iOS.

Pożądany rezultat: Architektura bezpieczeństwa przedsiębiorstwa powinna zablokować instalację nieautoryzowanych profili konfiguracji (iOS) lub certyfikatów CA (Android). Alternatywnie, architektura zabezpieczeń może wykryć obecność

nieautoryzowanych profili konfiguracji lub certyfikatów CA i wykonać inną odpowiednią akcję, taką jak zablokowanie urządzeniu dostępu do zasobów przedsiębiorstwa do czasu usunięcia profilu konfiguracji lub certyfikatu CA. Architektura powinna również wykrywać próby ataków typu „person-in-the-middle".

Zaobserwowany rezultat: Usługa Lookout wykryła atak typu „person-in-the-middle", zarówno na urządzeniach z systemem iOS, jak i Android. Wykryła również nieznany profil konfiguracji w systemie iOS.

5.2.7. ZDARZENIE POWODUJĄCE ZAGROŻENIE 7 — UTRATA POUFNOŚCI WRAŻLIWYCH INFORMACJI POPRZEZ PODSŁUCHIWANIE NIEZASZYFROWANEJ KOMUNIKACJI URZĄDZENIA

Podsumowanie: Złośliwe podmioty mogą z łatwością podsłuchiwać komunikację za pośrednictwem niezaszyfrowanych sieci bezprzewodowych, takich jak publiczne punkty dostępu Wi-Fi, które są powszechnie dostępne w kawiarniach i hotelach. Jeśli urządzenie jest podłączone do takiej sieci, złośliwy podmiot może uzyskać nieautoryzowany dostęp do wszelkich danych wysyłanych lub odbieranych przez urządzenie dla każdej sesji, która nie jest chroniona przez szyfrowanie w warstwie transportowej lub aplikacji.

Działanie testowe: Sprawdzenie, czy aplikacje będą próbowały nawiązać połączenie http lub nieszyfrowane.

Pożądany rezultat: Otrzymanie ostrzeżenia, gdy aplikacja próbuje nawiązać niezaszyfrowane połączenie lub uniemożliwienie jej tego.

Usługa Appthority może określić, czy aplikacje będą próbowały nawiązać połączenie http lub nieszyfrowane.

Systemy iOS i Android również mogą wymagać od aplikacji bezpiecznego połączenia. Gdy spróbuje ona połączyć się z serwerem i połączenie to będzie niezaszyfrowane, zostanie ono po prostu przerwane.

Zaobserwowany rezultat: Zarówno na systemie iOS, jak i Android, usługa Appthority wykryła zagrożenie „sends data unencrypted" (wysyła niezaszyfrowane dane) dla aplikacji. Przesyłanie danych za pośrednictwem nieszyfrowanych połączeń może spowodować utratę poufności informacji przesyłanych przez daną aplikację.

5.2.8. ZDARZENIE POWODUJĄCE ZAGROŻENIE 8 — NARUSZENIE INTEGRALNOŚCI URZĄDZENIA POPRZEZ ZASTOSOWANIE KODU ODBLOKOWUJĄCEGO, KTÓRY ZOSTAŁ ZAOBSERWOWANY, WYWNIOSKOWANY LUB POZYSKANY NA DRODZE ATAKU SIŁOWEGO

Podsumowanie: Złośliwy podmiot może pozyskać kod odblokowujący urządzenie użytkownika poprzez jego bezpośrednią obserwację, atak kanałem bocznym lub atak siłowy.

Działanie testowe:

- Próba całkowitego usunięcia kodu odblokowującego urządzenie. Sprawdzenie, czy próba się powiodła.
- Próba ustawienia kodu odblokowującego urządzenie na „1234", słaby czterocyfrowy osobisty numer identyfikacyjny (*ang. Personal Identification Number – PIN*). Sprawdzenie, czy próba się powiodła.
- Podejmowanie ciągłych prób odblokowania urządzenia i sprawdzenie, czy urządzenie zostało przywrócone do ustawień fabrycznych po 10 nieudanych próbach.

Pożądany rezultat: Zasady ustawione na urządzeniu przez system EMM (MobileIron) powinny wymagać ustawienia kodu odblokowującego urządzenie, uniemożliwiać jego usunięcie, wymagać jego minimalnej złożoności i przywracać urządzenie do ustawień fabrycznych po 10 nieudanych próbach odblokowania.

Ponadto usługa Lookout może identyfikować i zgłaszać urządzenia z wyłączonym ekranem blokady.

Zaobserwowany rezultat: W narzędziu MobileIron została zastosowana zasada wymuszająca korzystanie z kodu PIN na urządzeniach i przywrócenie

ustawień fabrycznych po 10 nieudanych próbach odblokowania urządzenia. Ponadto Lookout zgłasza, gdy urządzenie ma wyłączony ekran blokady. W przypadku obu urządzeń wszystkie dane zostały usunięte po 10 nieudanych próbach odblokowania.

Opcja usunięcia odblokowującego kodu PIN / kodu dostępu została wyłączona. Przy próbie ustawienia kodu PIN zawierającego powtarzające się lub kolejne znaki, wyświetlany był błąd informujący użytkownika, że nie może użyć wprowadzonego kodu PIN.

5.2.9. ZDARZENIE POWODUJĄCE ZAGROŻENIE 9 — NIEAUTORYZOWANY DOSTĘP DO USŁUG ZAPLECZA POPRZEZ LUKI W UWIERZYTELNIANIU LUB PRZECHOWYWANIU DANYCH UWIERZYTELNIAJĄCYCH W WEWNĘTRZNIE OPRACOWANYCH APLIKACJACH

Podsumowanie: Jeśli złośliwy podmiot uzyska nieautoryzowany dostęp do urządzenia mobilnego, atakujący ma również dostęp do znajdujących się na nim danych i aplikacji. Urządzenie mobilne może zawierać wewnętrzne aplikacje organizacji, które dają dostęp do wrażliwych danych lub usług zaplecza.

Działanie testowe: Aplikacja została przesłana do usługi Appthority w celu przeanalizowania podatności w zakresie danych uwierzytelniających.

Pożądany rezultat: Wykrycie i zgłoszenie słabości w zakresie danych uwierzytelniających.

Zaobserwowany rezultat: Usługa Appthority wykryła dane uwierzytelniające zapisane w kodzie aplikacji.

Korzystanie z danych uwierzytelniających zapisanych w kodzie aplikacji może stanowić podatność, jeśli zostaną one wykorzystane do uzyskania dostępu do zasobów przedsiębiorstwa przez nieautoryzowane podmioty. Jeśli dane uwierzytelniające zapisane w kodzie aplikacji zostaną zastosowane do jej zasady, zasada ta zostanie przypisana jako etykieta w systemie MobileIron do wszystkich urządzeń z zainstalowaną aplikacją.

5.2.10. ZDARZENIE POWODUJĄCE ZAGROŻENIE 10 — NIEAUTORYZOWANY DOSTĘP DO ZASOBÓW PRZEDSIĘBIORSTWA Z URZĄDZENIA NIEZARZĄDZANEGO I NARAŻONEGO NA NARUSZENIE BEZPIECZEŃSTWA

Podsumowanie: Pracownik, który uzyskuje dostęp do zasobów przedsiębiorstwa z niezarządzanego urządzenia mobilnego, naraża przedsiębiorstwo na skutki podatności, które mogą obejmować naruszenie bezpieczeństwa danych firmy. W przypadku urządzeń niezarządzanych nie są wykorzystywane mechanizmy bezpieczeństwa wdrożone przez organizację, takie jak: ochrona przed zagrożeniami mobilnymi, analiza zagrożeń mobilnych, usługi weryfikacji aplikacji i zasady bezpieczeństwa mobilnego. W przypadku takich niezarządzanych urządzeń organizacja ma ograniczony wgląd w ich stan — również w sytuacji, gdy ich bezpieczeństwo zostanie naruszone przez atakującego.

Działanie testowe: Próba bezpośredniego dostępu do usług przedsiębiorstwa, np. serwera poczty Exchange lub firmowej sieci VPN, z urządzenia mobilnego, które nie jest zarejestrowane w systemie EMM.

Pożądany rezultat: Usługi przedsiębiorstwa nie powinny być dostępne z urządzeń, które nie są zarejestrowane w systemie EMM. W przeciwnym razie przedsiębiorstwo nie jest w stanie skutecznie zarządzać urządzeniami w celu zapobiegania zagrożeniom.

Zaobserwowany rezultat: Urządzenia, które nie były zarejestrowane w systemie MobileIron, nie mogły uzyskać dostępu do zasobów przedsiębiorstwa, ponieważ brama VPN GlobalProtect uniemożliwiała ich uwierzytelnianie bez odpowiednich certyfikatów klienta. Certyfikaty klienta można uzyskać tylko poprzez rejestrację w systemie EMM.

5.2.11. ZDARZENIE POWODUJĄCE ZAGROŻENIE 11 — UTRATA DANYCH ORGANIZACJI Z POWODU ZGUBIENIA LUB KRADZIEŻY URZĄDZENIA

Podsumowanie: Ze względu na niewielkie rozmiary, urządzenia mobilne mogą zostać zgubione lub skradzione. Złośliwy podmiot, który uzyska fizyczną kontrolę nad

urządzeniem z nieodpowiednimi zabezpieczeniami, może uzyskać nieautoryzowany dostęp do wrażliwych danych lub zasobów dostępnych dla tego urządzenia.

Działanie testowe: Próba pobrania danych firmowych na urządzenie mobilne, które nie jest zarejestrowane w systemie EMM (można wykonać w połączeniu z TE-10). Próba usunięcia (w połączeniu z TE-8) kodu odblokowującego urządzenie lub wykazanie, że urządzenie nie ma kodu odblokowującego. Próba zlokalizowania i wyczyszczenia pamięci urządzenia za pomocą konsoli systemu EMM (nie powiedzie się, jeśli urządzenie nie jest w nim zarejestrowane).

Pożądany rezultat: Powinno być możliwe zlokalizowanie lub wyczyszczenie pamięci urządzeń zarejestrowanych w systemie EMM w odpowiedzi na zgłoszenie, że zostały one zgubione lub skradzione. Jak pokazano w TE-10, tylko urządzenia zarejestrowane w systemie EMM powinny mieć dostęp do zasobów przedsiębiorstwa. Jak pokazano w TE-8, zarejestrowanie urządzenia w systemie EMM może wymuszać blokadę ekranu z hasłem o odpowiedniej sile, co zapobiega jego niewłaściwemu wykorzystaniu (w tym utracie danych organizacji) w przypadku zgubienia lub kradzieży.

Jeśli urządzenie będzie niedostępne dla systemu EMM (np. odłączone od wszystkich sieci), dane kontrolne systemu EMM i dane firmowe zostaną usunięte po 10 nieudanych próbach odblokowania.

Zaobserwowany rezultat (zarejestrowane urządzenia): Zarejestrowane urządzenia są chronione. Została w nich zastosowana zasada przedsiębiorstwa wymagająca osobistego numeru identyfikacyjnego/ekranu blokady, dlatego nie można uzyskać dostępu do danych przedsiębiorstwa. Po 10 próbach uzyskania dostępu pamięć urządzenia została wymazana. Ponadto pamięć urządzenia została zdalnie wymazana po tym, jak zostało ono zgłoszone jako utracone w systemie zarządzania urządzeniami mobilnymi w przedsiębiorstwie.

Zaobserwowany rezultat (niezarejestrowane urządzenia): Jak wynika ze zdarzenia powodującego zagrożenie nr 10, tylko zarejestrowane urządzenia mogą uzyskać dostęp do usług przedsiębiorstwa. Gdy urządzenie próbowało uzyskać dostęp do

danych przedsiębiorstwa, połączenie z jego usługami nie było dostępne. Ponieważ urządzenie nie może uzyskać dostępu do przedsiębiorstwa, firmowe dane nie mogą się na nim znaleźć.

5.2.12. ZDARZENIE POWODUJĄCE ZAGROŻENIE 12 — UTRATA POUFNOŚCI DANYCH ORGANIZACJI Z POWODU ICH NIEAUTORYZOWANEGO PRZECHOWYWANIA W USŁUGACH NIEZARZĄDZANYCH PRZEZ ORGANIZACJĘ

Podsumowanie: Jeśli pracownik naruszy zasady zarządzania danymi, korzystając z niezarządzanych usług do przechowywania wrażliwych danych organizacji, dane te znajdą się poza jej kontrolą i nie będzie ona już w stanie chronić ich poufności, integralności ani dostępności. Złośliwe podmioty, które naruszą bezpieczeństwo nieautoryzowanego konta usługi lub dowolnego systemu obsługującego to konto, mogą uzyskać nieautoryzowany dostęp do danych.

Działanie testowe: Połączenie się z siecią VPN przedsiębiorstwa. Otwarcie strony internetowej lub aplikacji przedsiębiorstwa. Próba wyodrębnienia danych przedsiębiorstwa poprzez zrobienie zrzutu ekranu lub skopiowanie/wklejenie ich i wysłanie za pośrednictwem niezarządzanego konta e-mail.

Pożądany rezultat: Podczas korzystania z zarządzanych aplikacji zrzuty ekranu i inne działania związane z udostępnianiem danych będą zabronione przez system EMM.

Zaobserwowany rezultat: Za pomocą zasad ograniczeń i blokad w systemie, MobileIron administrator uniemożliwił następujące działania na urządzeniach:

Android

- kopiuj/wklej
- zrzut ekranu
- przesyłanie danych przez komunikację zbliżeniową
- transfer danych przez port USB
- Bluetooth

iOS

- wykonywanie zrzutów i nagrywanie ekranu (iOS 9+)
- AirDrop
- iCloud Backup
- dokumenty iCloud i dostęp do danych
- przechowywanie danych w usłudze iCloud przez zarządzane aplikacje
- przepływ danych między aplikacjami zarządzanymi i niezarządzanymi
- przekazanie danych między urządzeniami używającymi tego samego konta (*ang. hand-off*)

Ograniczenia te uniemożliwiły użytkownikowi skorzystanie z typowych sposobów wycieku danych.

5.3. SCENARIUSZE I USTALENIA

Jeden z aspektów naszej oceny bezpieczeństwa obejmował sprawdzenie, jak dobrze projekt referencyjny odpowiada charakterystyce bezpieczeństwa, którą miał zapewnić. Podkategorie ram cyberbezpieczeństwa zostały wykorzystane do zapewnienia struktury szacowania bezpieczeństwa poprzez odniesienie się do konkretnych punktów każdego standardu, które są cytowane w odniesieniu do podkategorii.

Przytoczone punkty zawierają elementy podlegające walidacji, których można oczekiwać od przykładowego rozwiązania. Wykorzystanie podkategorii ram cyberbezpieczeństwa jako podstawy organizacji naszej analizy pozwoliło nam systematycznie sprawdzać, jak dobrze projekt referencyjny spełnia zamierzone cechy bezpieczeństwa.

W tym punkcie przedstawiono scenariusze i ustalenia dotyczące cech bezpieczeństwa i prywatności, które miały być realizowane przez przykładowe rozwiązanie. Obejmuje on:

- opracowanie zestawienia ram cyberbezpieczeństwa i ram NICE;
- scenariusze zdarzeń powodujących zagrożenia i środki zaradcze w architekturze przykładowego rozwiązania;
- scenariusze działań na danych i potencjalne środki zaradcze, które organizacje mogą zastosować.

5.3.1. ZESTAWIENIE RÓL ROBOCZYCH Z RAM CYBERBEZPIECZEŃSTWA I RAM NICE

Podczas opracowywania przykładowego rozwiązania opracowano również zestawienie podkategorii ram cyberbezpieczeństwa w formie tabeli dla organizacji wdrażających możliwości przykładowego rozwiązania.

W miarę jak produkty przykładowego rozwiązania były instalowane, konfigurowane i wykorzystywane w jego architekturze, określono i dokumentowano funkcje przykładowego rozwiązania i odpowiadające im podkategorie ram cyberbezpieczeństwa, wraz z innymi wytycznymi.

Zestawienie to stało się ważnym zasobem dla przykładowego rozwiązania zawartego w tym przewodniku po praktykach, ponieważ zapewnia możliwość przekazania interesariuszom z ramienia organizacji informacji na temat środków bezpieczeństwa, którym przykładowe rozwiązanie może zaradzić, a także wymagań dotyczących pracowników wiążących się z wdrażaniem przykładowego rozwiązania.

Zestawienie produktów, środków bezpieczeństwa i wymagań dotyczących pracowników związanych z przykładowym rozwiązaniem znajduje się w tabeli I-1.

5.3.2. SCENARIUSZE I USTALENIA ZWIĄZANE ZE ZDARZENIAMI POWODUJĄCYMI ZAGROŻENIA

W ramach ustaleń przeciwdziałano zdarzeniom powodującym zagrożenia w przykładowej architekturze rozwiązania przy użyciu koncepcji i technologii przedstawionych w tabeli 5-1. Każde zdarzenie powodujące zagrożenie zostało zestawione z funkcjami, które umożliwiły złagodzenie związanego z nim ryzyka.

Uwaga: Choć nie zostało to przedstawione w tabeli, moduł TEE zapewnił odporne na manipulacje funkcje środowiska przetwarzania, które umożliwiły przeciwdziałanie zagrożeniom związanym z uruchamianiem urządzeń mobilnych i pamięcią w przykładowym rozwiązaniu.

Tabela 5-1 Zestawienie scenariuszy i ustaleń związanych ze zdarzeniami powodującymi zagrożenia

Zdarzenie powodujące zagrożenie	Sposób, w jaki architektura przykładowego rozwiązania umożliwia przeciwdziałanie zdarzeniu powodującemu zagrożenie	Funkcja technologii umożliwiająca przeciwdziałanie zdarzeniu powodującemu zagrożenie
Zdarzenie powodujące zagrożenie 1: Nieautoryzowany dostęp do wrażliwych informacji za pośrednictwem złośliwej lub naruszającej prywatność aplikacji.	Zapewnienie administratorom uzyskania informacji, do jakich danych firmowych mają dostęp aplikacje.	MTI
Zdarzenie powodujące zagrożenie 2: Kradzież danych uwierzytelniających poprzez kampanię wyłudzania informacji za pośrednictwem wiadomości SMS lub e-mail.	Wykorzystanie usługi PAN-DB do blokowania znanych złośliwych stron internetowych.	Zapora sieciowa
Zdarzenie powodujące zagrożenie 3: Złośliwe aplikacje zainstalowane za pośrednictwem adresów URL w wiadomościach SMS lub e-mail.	Zablokowanie możliwości instalowania aplikacji z nieznanych źródeł.	EMM
Zdarzenie powodujące zagrożenie 4: Utrata poufności i integralności w wyniku wykorzystania znanej podatności w systemie operacyjnym lub oprogramowaniu układowym.	Poddanie kwarantannie urządzenia niezgodnego z zasadami do czasu aktualizacji jego systemu operacyjnego.	EMM
Zdarzenie powodujące zagrożenie 5: Naruszenie prywatności poprzez niewłaściwe wykorzystanie czujników urządzenia.	Raporty z weryfikacji aplikacji informujące o czujnikach, do których aplikacja żądała dostępu.	MTI
Zdarzenie powodujące zagrożenie 6: Naruszenie integralności urządzenia lub jego komunikacji sieciowej poprzez instalację złośliwego systemu EMM/MDM, sieci, profili VPN lub certyfikatów.	Wykrycie ataku typu „*person-in-the-middle*” i nieautoryzowanego profilu konfiguracyjnego w systemie iOS.	MTD
Zdarzenie powodujące zagrożenie 7: Utrata poufności wrażliwych informacji poprzez podsłuchiwanie niezaszyfrowanej komunikacji urządzenia.	Raporty z weryfikacji aplikacji informujące, że dana aplikacja wysłała dane bez odpowiedniego szyfrowania.	Weryfikacja aplikacji
Zdarzenie powodujące zagrożenie 8: Naruszenie integralności urządzenia poprzez zastosowanie kodu odblokowującego, który został zaobserwowany, wywnioskowany lub pozyskany na drodze ataku siłowego.	Zastosowanie obowiązkowego czyszczenia pamięci urządzenia po 10 nieudanych próbach odblokowania.	EMM

Zdarzenie powodujące zagrożenie	Sposób, w jaki architektura przykładowego rozwiązania umożliwia przeciwdziałanie zdarzeniu powodującemu zagrożenie	Funkcja technologii umożliwiająca przeciwdziałanie zdarzeniu powodującemu zagrożenie
Zdarzenie powodujące zagrożenie 9: Nieautoryzowany dostęp do usług zaplecza poprzez luki w uwierzytelnianiu lub przechowywaniu danych uwierzytelniających w wewnętrznie opracowanych aplikacjach.	Raporty z weryfikacji aplikacji informujące, czy aplikacja wykorzystywała dane uwierzytelniające w niewłaściwy sposób.	MTI
Zdarzenie powodujące zagrożenie 10: Nieautoryzowany dostęp do zasobów przedsiębiorstwa z urządzenia niezarządzanego i narażonego na naruszenie bezpieczeństwa.	Urządzenia niezarejestrowane w systemie EMM nie były w stanie połączyć się z firmową siecią VPN.	VPN
Zdarzenie powodujące zagrożenie 11: Utrata danych organizacji z powodu zgubienia lub kradzieży urządzenia.	Dane przedsiębiorstwa były chronione przez egzekwowane zasady dotyczące kodów dostępu i możliwość wymazywania pamięci urządzeń.	EMM
Zdarzenie powodujące zagrożenie 12: Utrata poufności danych organizacji z powodu ich nieautoryzowanego przechowywania w usługach niezarządzanych przez organizację.	Zasady wymuszające zapobieganie utracie danych zostały wdrożone na urządzeniach.	EMM

5.3.3. SCENARIUSZE I USTALENIA ZWIĄZANE Z DZIAŁANIAMI NA DANYCH

Wyniki analizy PRAM wykazały, że trzy działania związane z danymi były szczególnie istotne dla projektu. Potencjalne środki zaradcze, które mogłyby zostać wykorzystane przez organizację w celu zmniejszenia ich skutków, zostały zidentyfikowane w ramach PRAM, jak pokazano poniżej. Więcej szczegółowych informacji na temat ustaleń z analizy PRAM można znaleźć w załączniku G.

Tabela 5-2 Zestawienie scenariuszy i ustaleń związanych z działaniami na danych

Działanie na danych	Opis działania na danych	Sposoby przeciwdziałania skutkom działań na danych
Działanie na danych 1: Blokowanie dostępu i wymazywanie pamięci urządzeń	Pracownicy najprawdopodobniej używają swoich urządzeń zarówno do celów osobistych, jak i związanych z pracą. Dlatego, jeśli w systemie jest możliwość całkowitego wymazania pamięci urządzenia, może dojść do utraty osobistych danych przez pracowników.	Zablokowanie dostępu urządzenia do zasobów przedsiębiorstwa do czasu ponownego przyznania uprawnień dostępu. Selektywne wymazywanie elementów pamięci urządzenia bez usuwania wszystkich znajdujących się na nim danych. Zalecanie pracownikom tworzenia kopii zapasowych osobistych danych przechowywanych na urządzeniach. Ograniczenie pracownikom możliwości wymazywania danych lub blokowania dostępu.
Działanie na danych 2: Monitorowanie pracowników	W sieciach należących do pracodawcy lub przez niego kontrolowanych wszelkie działania są stale monitorowane. Pracownicy mogą nie być świadomi monitorowania ich interakcji z systemem i mogą nie chcieć, aby takie monitorowanie miało miejsce.	Ograniczenie możliwości przeglądania danych dotyczących pracowników i ich urządzeń przez personel. Opracowanie zasad i technik organizacji mających na celu ograniczenie gromadzenia określonych elementów danych. Opracowanie zasad i technik organizacji dotyczących usuwania danych osobowych.
Działanie na danych 3: Udostępnianie danych między stronami	Przesyłanie danych o osobach i ich urządzeniach między różnymi stronami może być kłopotliwe dla pracowników, którzy mogą nie wiedzieć, kto ma dostęp do różnych informacji na ich temat.	Opracowanie zasad i technik organizacji w zakresie anonimizacji danych. Stosowanie szyfrowania. Ograniczenie lub wyłączenie dostępu do danych. Opracowanie zasad i technik organizacji mających na celu ograniczenie gromadzenia określonych elementów danych. Korzystanie z umów w celu ograniczenia przetwarzania danych przez strony trzecie.

6. WNIOSKI

Niniejszy dokument zawiera przegląd ram zarządzania ryzykiem i metodologii szacowania ryzyka dotyczącym prywatności, wyjaśnienie koncepcji bezpieczeństwa urządzeń mobilnych oraz przykładowe rozwiązanie dla organizacji wdrażających model COPE.

Nasza fikcyjna organizacja Orvilia Development rozpoczęła działalność z infrastrukturą urządzeń mobilnych, w której brakowało koncepcji architektury bezpieczeństwa dla tych urządzeń. Zastosowano metody zarządzania ryzykiem dla bezpieczeństwa i szacowania ryzyka dla prywatności, aby poznać obecne luki w architekturze i metody zwiększania bezpieczeństwa i prywatności systemów.

Po zidentyfikowaniu głównych zdarzeń powodujących zagrożenia na podstawie szacowania ryzyka, zastosowano odpowiednie technologie bezpieczeństwa dla urządzeń mobilnych. Obejmowały one lokalne rozwiązanie EMM zintegrowane z technologiami bezpieczeństwa mobilnego opartymi na chmurze i agentach, które umożliwiły wdrożenie zestawu funkcji bezpieczeństwa i prywatności wspierających scenariusz użytkowania.

Przewodnik po praktykach zawiera również w Tomie C (NIST SP 1800-21C) serię instrukcji krok po kroku obejmujących wstępne procesy (instalowanie lub udostępnianie) i konfigurowanie dla każdego elementu architektury, aby ułatwić inżynierom ds. bezpieczeństwa szybkie wdrożenie i ocenę naszego przykładowego rozwiązania w ich środowisku testowym.

W przykładowym rozwiązaniu naszego projektu referencyjnego wykorzystano standardowe produkty dostępne na rynku. Może ono być wykorzystane bezpośrednio przez dowolną organizację realizującą scenariusz COPE poprzez wdrożenie infrastruktury bezpieczeństwa, która umożliwi integrację lokalnych i hostowanych w chmurze mobilnych technologii bezpieczeństwa. Przewodnik po praktykach zawiera projekt referencyjny i przykładowe rozwiązanie, które organizacja może wykorzystać w całości lub w części jako podstawę do stworzenia rozwiązania niestandardowego, zapewniającego właściwości w zakresie bezpieczeństwa i prywatności, które najlepiej wspomagają realizację jej unikalnego scenariusza użytkowania urządzeń mobilnych.

7. UWAGI DOTYCZĄCE KOLEJNYCH PROJEKTÓW

Interesującym tematem dla przyszłego projektu jest scenariusz „przynieś własne urządzenie” (*ang. Bring Your Own Device – BYOD*). Wiąże się on z koniecznością ochrony danych firmowych na urządzeniach należących do pracowników, których będą oni używać zarówno do pracy, jak i do celów prywatnych. Innym obszarem zainteresowania jest oprogramowanie typu „cienki klient” (*ang. thin client*) wdrażane na urządzeniach mobilnych, umożliwiające pracownikowi dostęp do urządzenia wirtualnego znajdującego się w infrastrukturze firmowej.

Co więcej, analiza pojawiających się technologii 5G w odniesieniu do bezpieczeństwa urządzeń mobilnych jest nową dziedziną, która stwarza szerokie możliwości badawcze.

ZAŁĄCZNIK A AKRONIMY

Wybrane akronimy i skróty użyte w treści niniejszego opracowania zostały rozwinięte i zdefiniowane poniżej.

Dodatkowo patrz: *NSC 7298, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*

Akronim	Terminologia angielska	Terminologia polska
AD	Active Directory	Usługa Active Directory
ADCS	Active Directory Certificate Services	Usługi ADCS
ADDS	Active Directory Domain Services	Usługi ADDS
API	Application Programming Interface	Interfejs programistyczny aplikacji
ATARC	Advanced Technology Academic Research Center	Akademickie Centrum Badań nad Zaawansowanymi Technologiami
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge	Taktyki, techniki i powszechna wiedza atakujących
BYOD	Bring Your Own Device	Przynieś własne urządzenie
CIO	Chief Information Officer	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za technologie informacyjne
CIS	Center for Internet Security	Centrum ochrony w Internecie
COMSEC	Communications Security	Bezpieczeństwo komunikacji
COPE	Corporate-Owned Personally-Enabled	Własność firmy dostępna prywatnie
CSP	Credential Service Provider	Dostawca usług uwierzytelniania
CVE	Common Vulnerabilities and Exposures	Typowe podatności i zagrożenia
DHS	Department of Homeland Security	Departament Bezpieczeństwa Wewnętrznego
DMZ	Demilitarized Zone	Strefa zdemilitaryzowana
EMM	Enterprise Mobility Management	Zarządzanie mobilnością w przedsiębiorstwie
FedRAMP	Federal Risk and Authorization Management Program	Federalny program zarządzania ryzykiem i autoryzacją
FIPS	Federal Information Processing Standards	Federalne standardy przetwarzania informacji
GPS	Global Positioning System	Globalny system pozycjonowania
HTTP	Hypertext Transfer Protocol	Protokół http
HTTPS	Hypertext Transfer Protocol Secure	Protokół https

IEC	International Electrotechnical Commission	Międzynarodowa Komisja Elektrotechniczna
IEEE	Institute of Electrical and Electronics Engineers	Instytut Inżynierów Elektryków i Elektroników
IMEI	International Mobile Equipment Identity	Międzynarodowy identyfikator urządzenia mobilnego
IP	Internet Protocol	Protokół internetowy
IR	Interagency Report	Sprawozdanie międzyresortowe
ISO	International Organization for Standardization	Międzynarodowa organizacja normalizacyjna
IT	Information Technology	Technologia informacyjna
MDM	Mobile Device Management	Zarządzanie urządzeniami mobilnymi
MSCT	Mobile Services Category Team	Zespół ds. kategorii usług mobilnych
MTC	Mobile Threat Catalogue	Katalog zagrożeń urządzeń mobilnych
MTD	Mobile Threat Defense	Obrona przed zagrożeniami urządzeń mobilnych
MTI	Mobile Threat Intelligence	Analiza zagrożeń urządzeń mobilnych
MTP	Mobile Threat Protection	Ochrona przed zagrożeniami urządzeń mobilnych
NCCoE	National Cybersecurity Center of Excellence	Krajowe centrum doskonałości w dziedzinie cyberbezpieczeństwa
NIAP	National Information Assurance Partnership	Krajowe partnerstwo w dziedzinie wiarygodności informacji
NICE	National Initiative for Cybersecurity Education	Krajowa inicjatywa na rzecz edukacji w zakresie cyberbezpieczeństwa
NIST	National Institute of Standards and Technology	Narodowy Instytut Standaryzacji i Technologii
NVD	National Vulnerability Database	Krajowa baza danych dotyczących podatności na zagrożenia
OS	Operating System	System operacyjny
PA	Palo Alto Networks	Paolo Alto Networks
PII	Personally Identifiable Information	Dane osobowe
PRAM	Privacy Risk Assessment Methodology	Metodologia szacowania ryzyka dla prywatności
RMF	Risk Management Framework	Ramy zarządzania ryzykiem
ROM	Read-only Memory	Pamięć tylko do odczytu, pamięć ROM

SCEP	Simple Certificate Enrollment Protocol	Prosty protokół rejestracji certyfikatów
SIEM	Security Information and Event Management	Bezpieczeństwo Informacji i Zarządzanie Zdarzeniami
SMS	Short Message Service	Usługa krótkich wiadomości tekstowych
SP	Special Publication	Publikacja specjalna
TE	Threat Event	Zdarzenie powodujące zagrożenie
TEE	Trusted Execution Environment	Zaufane środowisko wykonawcze
TLS	Transport Layer Security	Bezpieczeństwo warstwy transportowej
UPN	User Principal Name	Główna nazwa użytkownika
URL	Uniform Resource Locator	Standard URL
VPN	Virtual Private Network	Wirtualna sieć prywatna

ZAŁĄCZNIK B SŁOWNIK

Poniżej zostały przedstawione definicje wybranych terminów użytych w treści niniejszej publikacji. Niektóre definicje zostały opatrzone odnośnikami do źródeł.

Dodatkowo patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*

Terminologia angielska	Terminologia polska	Definicja
Access Management	Zarządzanie dostępem	Zarządzanie dostępem to zestaw praktyk, które umożliwiają dostęp do określonego zasobu tylko tym osobom, które mają do tego uprawnienia. Trzy najczęściej spotykane usługi zarządzania dostępem, z którymi można się zetknąć każdego dnia, być może nie zdając sobie z tego sprawy, to: administrowanie zasadami, uwierzytelnianie i autoryzacja [48].
Agent	Agent	Program systemu zapobiegania atakom opartego na hoście, który monitoruje i analizuje aktywność oraz wykonuje działania zapobiegawcze; program lub wtyczka, która umożliwia sieci VPN SSL dostęp do aplikacji i usług innych niż internetowe [49].
Application Layer	Warstwa aplikacji	Warstwa stosu protokołów TCP/IP, która wysyła i odbiera dane dla określonych aplikacji, takich jak DNS, HTTP i SMTP [49].
App-Vetting Process	Proces weryfikacji aplikacji	Proces weryfikacji, czy aplikacja spełnia wymagania bezpieczeństwa organizacji. Proces weryfikacji aplikacji obejmuje jej testowanie oraz działania związane z jej zatwierdzeniem lub odrzuceniem [50].
Brute-Force Attack	Atak siłowy	W kryptografii, atak polegający na wypróbowaniu wszystkich możliwych kombinacji w celu znalezienia dopasowania [51].
Chief Information Officers (CIO) Council	Rada kluczowych osób w jednostce organizacyjnej odpowiedzialnych za technologie informacyjne	Rada CIO jest głównym międzyresortowym forum mającym na celu poprawę praktyk agencji związanych z projektowaniem, pozyskiwaniem, rozwojem, modernizacją, wykorzystaniem, udostępnianiem i wydajnością federalnych zasobów informacyjnych [52].

Terminologia angielska	Terminologia polska	Definicja
Common Vulnerabilities and Exposures	Typowe podatności i zagrożenia	Słownik powszechnie znanych nazw podatności systemów informacyjnych [53].
Corporate-Owned Personally-Enabled (COPE)	Corporate-Owned Personally-Enabled COPE Organizacyjne urządzenia mobilne obsługiwane osobiście przez użytkowników	Urządzenie będące własnością przedsiębiorstwa i przydzielone pracownikowi. Zarówno przedsiębiorstwo, jak i pracownik mogą instalować aplikacje na urządzeniu.
Cryptographic Algorithm	Algorytm kryptograficzny	Ściśle określona procedura obliczeniowa, w ramach której pobierane są zmienne dane wejściowe, w tym klucz kryptograficzny, oraz generowane są dane wyjściowe [54].
Cryptographic Key	Klucz kryptograficzny	Wartość używana do kontrolowania operacji kryptograficznych, takich jak deszyfrowanie, szyfrowanie, generowanie podpisu lub weryfikacja podpisu. [55].
Cryptography	Kryptografia	Dyscyplina, która obejmuje zasady, środki i metody przekształcania danych w celu ukrycia ich semantycznej zawartości, zapobiegania ich nieautoryzowanemu użyciu lub zapobiegania ich niewykrytej modyfikacji [54].
Data Action	Działanie na danych	Operacje w systemie obejmujące przetwarzanie danych osobowych [20].
De-identification	Anonimizacja	Ogólny termin oznaczający dowolny proces usuwania powiązania między zestawem danych umożliwiających identyfikację a osobą, której dane dotyczą [51].
Demilitarized Zone (DMZ)	DMZ Strefa zdemilitaryzowana	Sieć utworzona przez połączenie dwóch zapór sieciowych. Systemy, które są dostępne z zewnątrz, ale wymagają pewnej ochrony, są zwykle zlokalizowane w sieciach DMZ [56].
Disassociability	Usunięcie powiązania	Umożliwienie przetwarzania danych osobowych lub zdarzeń bez powiązania z osobami lub urządzeniami wykraczającego poza wymagania operacyjne systemu [20].
Encryption	Szyfrowanie	Kryptograficzna transformacja danych umożliwiająca uzyskanie szyfrogramu [54].

Terminologia angielska	Terminologia polska	Definicja
Enterprise Mobility Management	Zarządzanie mobilnością w przedsiębiorstwie	Systemy zarządzania mobilnością w przedsiębiorstwie (EMM) są powszechnym sposobem zarządzania urządzeniami mobilnymi w firmach. Choć same w sobie nie są technologią bezpieczeństwa, systemy EMM umożliwiają wdrażanie zasad na puli urządzeń przedsiębiorstwa i monitorowanie ich stanu [9].
Identity Verification	Identyfikacja tożsamości	Potwierdzenie, poprzez dostarczenie obiektywnych dowodów, że określone wymogi zostały spełnione (np. wymogi dotyczące jednostki zostały prawidłowo zdefiniowane lub atrybuty jednostki zostały prawidłowo przedstawione; lub procedura lub funkcja działa zgodnie z przeznaczeniem i prowadzi do oczekiwanego rezultatu). Zaczerpnięto z definicji terminu „Weryfikacja” [54].
Impact	Wpływ	Skutki utraty poufności, integralności lub dostępności informacji lub systemu informacyjnego dla działalności organizacji, jej aktywów, osób fizycznych, innych organizacji lub państwa (w tym interesów bezpieczeństwa narodowego) [11].
Key Logger	Rejestrator klawiszy	Zdalny program służący do rejestrowania naciśniętych klawiszy na klawiaturze komputera w celu uzyskania haseł lub kluczy szyfrowania, a tym samym obejścia innych środków bezpieczeństwa [57].
Malware	Oprogramowanie złośliwe	Oprogramowanie – zwykłe lub układowe – służące do wykonania nieautoryzowanego procesu, który będzie miał negatywny wpływ na poufność, integralność lub dostępność systemu informacyjnego. Wirus, robak, koń trojański lub inna jednostka oparta na kodzie, która infekuje host. Oprogramowanie szpiegujące i niektóre formy programów typu adware również są przykładami złośliwych kodów [11].
Manageability	Umożliwianie zarządzania	Zapewnienie możliwości szczegółowego zarządzania danymi, w tym ich modyfikowania, usuwania i selektywnego ujawniania [20].

Terminologia angielska	Terminologia polska	Definicja
Mobile Device	Urządzenie mobilne	Przenośne urządzenie komputerowe, które: (I) mieści się w niewielkiej obudowie, dzięki czemu może być łatwo przenoszone przez jedną osobę; (II) zostało zaprojektowane do działania bez fizycznego połączenia (np. bezprzewodowego przesyłania lub odbierania informacji); (III) jest wyposażone w lokalną, niewymienną lub wymienną pamięć masową; oraz (IV) ma niezależne źródło zasilania. Urządzenia mobilne mogą być również wyposażone w funkcje komunikacji głosowej, wbudowane czujniki umożliwiające przechwytywanie informacji i/lub wbudowane funkcje synchronizacji danych lokalnych z lokalizacjami zdalnymi. Przykłady: smartfony, tablety, laptopy, e-czytniki [11].
Mobile Device Management (MDM)	Zarządzanie urządzeniami mobilnymi MDM	Administrowanie urządzeniami mobilnymi, takimi jak smartfony, tablety, komputery, laptopy i komputery stacjonarne. System MDM jest zwykle wdrażany przy użyciu produktu innej firmy posiadającego funkcje zarządzania dla poszczególnych producentów urządzeń mobilnych [50].
Network Layer	Network Layer Warstwa sieciowa	Warstwa stosu protokołów TCP/IP odpowiedzialna za routing pakietów w sieciach [49].
Person (Man)-in-the-Middle Attack	Atak typu person man-in-the-middle (MIM)	Atak, w ramach którego osoba atakująca znajduje się pomiędzy dwiema komunikującymi się stronami w celu przechwycenia i/lub zmiany danych przesyłanych między nimi. W kontekście uwierzytelniania atakujący może znajdować się między zgłaszającym a weryfikatorem, między rejestrującym a CSP podczas rejestracji lub między subskrybentem a CSP podczas wiązania uwierzytelniającego [55].

Terminologia angielska	Terminologia polska	Definicja
Phishing	Wyłudzanie informacji	Atak, w ramach którego subskrybent zostaje zwabiony (zazwyczaj za pośrednictwem wiadomości e-mail) do interakcji z fałszywym weryfikatorem i nakłoniony do ujawnienia informacji, które mogą zostać wykorzystane do podszycia się pod tego subskrybenta wobec prawdziwego weryfikatora [55].
Predictability	Przewidywalność	Umożliwienie osobom fizycznym, właścicielom i operatorom przyjmowania wiarygodnych założeń dotyczących danych i ich przetwarzania przez system, produkt lub usługę [20].
Predisposing Conditions	Warunki predysponujące	Stan istniejący w organizacji, misji/procesie biznesowym, architekturze przedsiębiorstwa lub systemie informacyjnym, w tym w jego środowisku operacyjnym, który wpływa na (tj. zwiększa lub zmniejsza) prawdopodobieństwo, że jedno lub więcej zdarzeń powodujących zagrożenie, po ich zainicjowaniu, doprowadzi do niepożądanych konsekwencji lub negatywnych skutków dla działalności i aktywów organizacji, osób fizycznych, innych organizacji lub państwa
Privacy Risk Assessment Methodology (PRAM)	Metodologia szacowania ryzyka dla prywatności PRAM	PRAM to narzędzie, w ramach którego stosowany jest model ryzyka z publikacji NISTIR 8062, umożliwiający organizacjom analizę, ocenę i ustalenie priorytetów zagrożeń dla prywatności w celu określenia sposobu reagowania i wyboru odpowiednich rozwiązań. PRAM może ułatwiać współpracę i komunikację między różnymi komponentami organizacji, w tym ochroną prywatności, cyberbezpieczeństwem, działalnością biznesową i personelem IT [58].
Read-Only Memory	Pamięć tylko do odczytu	ROM to wstępnie zapisany nośnik pamięci, z którego można jedynie odczytywać dane, ale nie można ich na nim zapisać [59].

Terminologia angielska	Terminologia polska	Definicja
Red Team Exercise	Warsztaty „Red Team”	Próba, w warunkach rzeczywistych, która jest przeprowadzana jako symulowany atak na misję organizacji i/lub procesy biznesowe w celu dokonania kompleksowej oceny zabezpieczeń systemu informatycznego i organizacji [11].
Replay Resistance	Odporność na odtwarzanie	Ochrona przed przechwyceniem przesłanych informacji uwierzytelniających lub kontroli dostępu i ich późniejszym ponownym przesłaniem z zamiarem wywołania nieautoryzowanego efektu lub uzyskania nieuprawnionego dostępu [60].
Risk	Ryzyko	Miara stopnia zagrożenia podmiotu przez potencjalną okoliczność lub zdarzenie. Zazwyczaj jest funkcją: (I) niekorzystnych skutków, które powstałyby w przypadku wystąpienia okoliczności lub zdarzenia oraz (II) prawdopodobieństwa ich wystąpienia [12].
Risk Assessment	Szacowanie ryzyka	Proces identyfikacji zagrożeń dla działalności organizacji (w tym misji, funkcji, wizerunku, reputacji), aktywów organizacji, osób fizycznych, innych organizacji i państwa, wynikających z działania systemu informacyjnego. Część zarządzania ryzykiem, obejmuje analizy zagrożeń i podatności na zagrożenia oraz uwzględnia środki zaradcze w postaci planowanych lub wprowadzonych zabezpieczeń. Synonim analizy ryzyka [11].
Risk Management Framework	Ramy zarządzania ryzykiem	Ramy zarządzania ryzykiem (RMF) zapewniają ustrukturyzowane, ale elastyczne podejście do zarządzania częścią ryzyka wynikającego z włączenia systemów do misji i procesów biznesowych organizacji [61].
Sandbox	Piaskownica	Ograniczone, kontrolowane środowisko wykonawcze, które uniemożliwia potencjalnie złośliwemu oprogramowaniu, takiemu jak kod mobilny, dostęp do jakichkolwiek zasobów systemowych z wyjątkiem tych, do których oprogramowanie jest uprawnione (w środowisku piaskownicy) [54].

Terminologia angielska	Terminologia polska	Definicja
Security Control	Środek bezpieczeństwa/ zabezpieczenie	Zabezpieczenie lub środek zaradczy przewidziany dla systemu informacyjnego lub organizacji, mający na celu ochronę poufności, integralności i dostępności informacji oraz spełnienie zestawu określonych wymogów bezpieczeństwa [11].
Side-Channel Attacks	Ataki kanałem bocznym	Atak umożliwiający wyciek informacji z fizycznego kryptosystemu. Cechy, które mogą zostać wykorzystane w ramach ataku kanałem bocznym, obejmują synchronizację, zużycie energii oraz emisje elektromagnetyczne i akustyczne [55].
Social Engineering	Inżynieria społeczna	Działanie polegające na nakłonieniu osoby fizycznej do ujawnienia wrażliwych informacji, udzielenia nieautoryzowanego dostępu lub popełnienia oszustwa poprzez nawiązanie kontaktu z tą osobą w celu zdobycia jej zaufania [55].
Threat	Zagrożenie	Wszelkie okoliczności lub zdarzenia mogące mieć negatywny wpływ na działalność organizacji (w tym misję, funkcje, wizerunek lub reputację), aktywa organizacji, osoby fizyczne, inne organizacje lub państwo za pośrednictwem systemu informacyjnego poprzez nieuprawniony dostęp, zniszczenie, ujawnienie, modyfikację informacji i/lub odmowę świadczenia usługi [12].
Threat Events	Zdarzenia powodujące zagrożenie	Zdarzenie lub sytuacja, która potencjalnie może spowodować niepożądane konsekwencje lub wpływ [12].
Threat Intelligence	Analiza zagrożeń	Informacje o zagrożeniach, które zostały zebrane, przekształcone, przeanalizowane, zinterpretowane lub wzbogacone w celu zapewnienia niezbędnego kontekstu dla procesów decyzyjnych [62].
Threat Sources	Źródło zagrożenia	Intencja i metoda ukierunkowane na celowe wykorzystanie podatności w zabezpieczeniach lub sytuacja i metoda, która może przypadkowo spowodować podatność na zagrożenie. Synonim: czynnik zagrożenia [11].

Terminologia angielska	Terminologia polska	Definicja
Transport Layer	Warstwa transportowa	Warstwa stosu protokołów TCP/IP odpowiedzialna za niezawodną, kompleksową komunikację połączeniową lub bezpołączeniową [49].
Transport Layer Security (TLS)	Bezpieczeństwo warstwy transportowej TLS	Protokół bezpieczeństwa zapewniający prywatność i integralność danych między dwiema komunikującymi się aplikacjami. Protokół składa się z dwóch warstw: TLS Record Protocol i TLS Handshake Protocol [54].
Trusted Certificate	Zaufany certyfikat	Certyfikat, któremu ufa strona ufająca na podstawie jego bezpiecznego i uwierzytelnionego transferu. Klucze publiczne zawarte w zaufanych certyfikatach są używane do uruchamiania ścieżek certyfikacji. Są również nazywane „kotwicami zaufania” [63].
Unmanaged Device	Niekontrolowane urządzenie	Urządzenie znajdujące się w zakresie oceny, które jest nieautoryzowane lub, jeśli jest autoryzowane, nie jest przypisane do administrowania [64].
Virtual Private Network	Wirtualna sieć prywatna	Chronione łącze systemu informacyjnego w ramach którego wykorzystywane jest tunelowanie, środki bezpieczeństwa i translacja adresów punktów końcowych, dające efekt dedykowanego łącza [54].
Vulnerability	Podatność	Słaby punkt w systemie informacyjnym, procedurach bezpieczeństwa systemu, wewnętrznych środkach bezpieczeństwa lub wdrożeniu, który może zostać wykorzystany przez źródło zagrożenia [12].
Watering Hole	Atak typu „watering hole”	Ataki typu *watering hole* polegają na naruszeniu bezpieczeństwa jednej lub więcej autentycznych witryn internetowych za pomocą złośliwego oprogramowania w celu zainfekowania urządzeń odwiedzających te witryny osób [65].

ZAŁĄCZNIK C REFERENCJE

	NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[7]
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800-46	Przewodnik po telepracy w podmiocie publicznym. Zdalny dostęp i bezpieczeństwo używania prywatnych urządzeń (BYOD)
NSC 800-52	Wskazówki dotyczące wyboru, konfigurowania i wykorzystania implementacji TLS (Transport Layer Security)
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61
NSC 800-161	Praktyki zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw dla systemów i organizacji – na podstawie NIST SP 800-161
NSC 800-209	Rekomendacje w zakresie bezpieczeństwa infrastruktury pamięci masowych

[7] Narodowe Standardy Cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl (www.gov.pl)

	PUBLIKACJE ANGLOJĘZYCZNE
[1]	National Institute of Standards and Technology (NIST), "NIST Computer Security Resource Center," [Online]. Available: https://csrc.nist.gov/publications/sp800.
[2]	National Information Assurance Partnership (NIAP), "NIAP Home Page," [Online]. Available: https://www.niap-ccevs.org/.
[3]	Department of Homeland Security, "Home Page," [Online]. Available: https://www.dhs.gov/.
[4]	Federal Chief Information Officers (CIO) Council, "Federal CIO Home Page," [Online]. Available: https://www.cio.gov/.
[5]	National Institute of Standards and Technology (NIST), "NIST Cybersecurity Framework, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," 16 April 2018. [Online]. Available: https://www.nist.gov/cyberframework.
[6]	National Institute of Standards and Technology (NIST), "NIST Privacy Engineering Program," [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.
[7]	National Institute of Standards and Technology (NIST), "NIST SP 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," August 2017. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-181/final.
[8]	National Institute of Standards and Technology (NIST), "Risk Management Framework (RMF) Overview," [Online]. Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview.
[9]	National Institute of Standards and Technology (NIST), "Mobile Threat Catalogue," [Online]. Available: https://pages.nist.gov/mobile-threat-catalogue/.
[10]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Mobile Device Security for Enterprises Building Block Version 2 Final Draft," 12 September 2014. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/mds-project-description-final.pdf.
[11]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," 22 January 2015. [Online]. Available: https://csrc.nist.gov/publications/sp.
[12]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments," September 2012. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[13]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-124 Revision 2 Draft, Guidelines for Managing the Security of Mobile Devices in the Enterprise," March 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft.
[14]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-4, Mobile Device Security: Cloud and Hybrid Builds," 21 February 2019. [Online]. Available: https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid.
[15]	International Organization for Standardization / International Electrotechnical Commission / Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE), "International Organization for Standardization / International Electrotechnical Commission / Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, Systems and software engineering System life cycle processes," 2015. [Online]. Available: https://www.iso.org/standard/63711.html.
[16]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 Volume 1: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," November 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800- 160/vol-1/final.
[17]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy," December 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.
[18]	Tech Times, "Flashlight apps are spying on users Android, iOS, Windows Phone smartphones, is yours on the list?," 26 October 2014. [Online]. Available: https://www.techtimes.com/articles/18762/20141026/flashlight-apps-are-spying-on-users-android-ios-windows-phone-smartphones-is-yours-on-the-list.htm.
[19]	National Institute of Standards and Technology (NIST), "NIST Privacy Framework," [Online]. Available: https://www.nist.gov/privacy-framework.
[20]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Internal Report (NISTIR) 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems," January 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.
[21]	M. A. A. B. Mohamed Sabt, "Trusted Execution Environment: What It is, and What It is Not. 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Helsinki, Finland," August 2015. [Online]. Copy and paste link into browser to access. Available: https://hal.archives-ouvertes.fr/hal-01246364/file/trustcom_2015_tee_what_it_is_what_it_is_not.pdf.
[22]	Zimperium, "MobileIron Threat Defense, Mobile Device Security & MDM," [Online]. Available: https://www.zimperium.com/partners/mobileiron.

[23]	National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile Protection Profile for Mobile Device Management Version 4.0," 25 April 2019. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm.
[24]	National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile Extended Package for VPN Gateways Version 2.1," 8 March 2017. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm.
[25]	National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile Collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314," 14 March 2018. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm.
[26]	National Information Assurance Partnership, "Approved Protection Profiles," [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm.
[27]	Qualcomm, "Qualcomm Secure Boot and Image Authentication Technical Overview," [Online]. Available: https://www.qualcomm.com/media/documents/files/secure-boot-and-image- authentication-technical-overview-v1-0.pdf.
[28]	National Information Assurance Partnership (NIAP), "Product Compliant List," [Online]. Available: https://www.niap-ccevs.org/Product/.
[29]	Palo Alto Networks, "Remote Access VPN (Certificate Profile)," [Online]. Available: https://docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/globalprotect-quick-configs/remote-access-vpn-certificate-profile.
[30]	MobileIron, "Admin Google Android Google Apps API," [Online]. Available: http://mi.extendedhelp.mobileiron.com/45/all/en/desktop/Google_Apps_API.htm.
[31]	MobileIron, "MobileIron unified endpoint security platform," [Online]. Available: https://www.mobileiron.com/en/unified-endpoint-management/platform.
[32]	Open Web Application Security Project (OWASP), [Online]. Available: https://www.owasp.org/index.php/Main Page.
[33]	Palo Alto Networks, "Always On VPN Configuration," [Online]. Available: https://docs.paloaltonetworks.com/globalprotect/7-1/globalprotect-admin/globalprotect-quick-configs/always-on-vpn-configuration.
[34]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," July 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final.
[35]	National Institute of Standards and Technology (NIST), "Cryptographic Module Validation Program," [Online]. Available: https://csrc.nist.gov/projects/cryptographic-module-validation- program.
[36]	Palo Alto Networks, "FIPS-CC Security Functions documentation site," [Online]. Available: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/certifications/fips-cc-security-functions.

[37]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52, Revision 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations," August 2019. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final.
[38]	Apple Computer, "Apple at Work," [Online]. Available: https://www.apple.com/business/it/.
[39]	Apple Computer, "Apple Configurator 2," [Online]. Available: https://itunes.apple.com/us/app/apple-configurator-2/id1037126344?mt=12.
[40]	Apple Computer, "Apple Platform Security," [Online]. Available: https://support.apple.com/guide/security/welcome/web.
[41]	Android.com, "Build a device policy controller," [Online]. Available: https://developer.android.com/work/dpc/build-dpc.
[42]	Android.com, "Work profiles on fully managed devices," [Online]. Available: https://developers.google.com/android/work/requirements/work-profile.
[43]	Google.com, "Android Enterprise Fully managed device," [Online]. Available: https://developers.google.com/android/work/requirements/fully-managed-device.
[44]	Google.com, "Android Enterprise Work profile," [Online]. Available: https://www.android.com/enterprise/.
[45]	International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), "ISO/IEC 27001:2013 Information technology -Security techniques - Information security management systems -Requirements," October 2013. [Online]. Available: https://www.iso.org/standard/54534.html.
[46]	Center for Internet Security, "Center for Internet Security Home Page," [Online]. Available: https://www.cisecurity.org/.
[47]	Google.com, "Google Play Store," [Online]. Available: https://play.google.com/store/apps.
[48]	IDManagement.gov, "Federal Identity, Credential, and Access Management Architecture," [Online]. Available: https://arch.idmanagement.gov/services/access/.
[49]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-113 Guide to SSL VPNs," July 2008. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-113/final.
[50]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-163 Revision 1, Vetting the Security of Mobile Applications," April 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf.

[51] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Internal Report (NISTIR) 8053, De-Identification of Personal Information," October 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.

[52] General Services Administration, "Chief Information Officers Council (CIOC)," [Online]. Available: https://www.gsa.gov/about-us/organization/office-of-governmentwide-policy/office-of-shared-solutions-and-performance-improvement/chief-information-officers-council-cioc.

[53] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-126 Revision 3, The Technical Specification for the Security Content Automation Protocol (SCAP)," February 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf.

[54] Committee on National Security Systems, "Committee on National Security Systems (CNSS) Glossary, Publication 4009," 6 April 2015. [Online]. Available: https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

[55] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, Digital Identity Guidelines," 2 March 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[56] National Institute of Standards and Technology (NIST), "NISTIR 7711 Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters," September 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7711.pdf.

[57] National Institute of Standards and Technology (NIST), "NIST Special Publication 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security," May 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[58] National Institute of Standards and Technology (NIST), "Risk Assessment Tools," [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/browse/risk-assessment-tools.

[59] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication 800-88, Revision 1, Guidelines for Media Sanitization," December 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

[60] National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Revision 2, Protecting Controlled Unclassified Information in Non-federal Systems and Organizations," February 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

[61]	National Institute of Standards and Technology (NIST), "Risk Management Framework: Quick Start Guide," [Online]. Available: https://csrc.nist.gov/projects/risk-management/risk- management-framework-quick-start-guides.
[62]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-150, Guide to Cyber Threat Information Sharing," October 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.
[63]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure," February 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf.
[64]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) 8011 Volume 1, Automation Support for Security Control Assessments," June 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8011-1.pdf.
[65]	United States Department of Homeland Security, "ICS-CERT Monitor," October, November, December 2013. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf.
[66]	National Institute of Standards and Technology (NIST), "Digital Identity Guidelines," 2 March 2020. [Online]. Available: https://csrc.nist.gov/publications/sp.
[67]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-114 Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security," July 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final.
[68]	Executive Office of the President, "Bring Your Own Device, a Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs," 23 August 2012. [Online]. Available: https://obamawhitehouse.archives.gov/digitalgov/bring-your-own-device.
[69]	Federal CIO Council and Department of Homeland Security, "Mobile Security Reference Architecture Version 1.0," 23 May 2013. [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Reference-Architecture.pdf.
[70]	Digital Services Advisory Group and Federal Chief Information Officers Council, "Government Use of Mobile Technology Barriers, Opportunities, and Gap Analysis," December 2012. [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Government_Mobile_Technology_Barriers_Opportunities and Gaps.pdf.
[71]	"Mobile Computing Decision," [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Decision-Framework-Appendix-B.pdf.

[72] Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC), "Mobility Strategy Development Guidelines Working Group Document," June 2017. [Online]. Available: https://hallways.cap.gsa.gov/app/#/gateway/mobile-services-category- team/9658/docs/12997/Agency_Mobility_Strategy_Deliverable.pdf.

[73] Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC), "Mobile Threat Protection App Vetting and App Security Working Group Document," July 2017. [Online]. Available: https://hallways.cap.gsa.gov/app/#/gateway/mobile-services- category-team/9658/docs/12996/Mobile_Threat_Protection_Deliverable.pdf.

[74] Mobile Services Category Team (MSCT), "Device Procurement and Management Guidance," November 2016. [Online]. Available: https://hallways.cap.gsa.gov/app/#/gateway/information-technology/4485/mobile-device-procurement-and-management-guidance.

[75] Mobile Services Category Team (MSCT), "Mobile Device Management (MDM) MDM Working Group Document," August 2017. [Online]. Available: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1197/2017/10/EMM_Deliverable.pdf.

[76] Mobile Services Category Team (MSCT), "Mobile Services Roadmap (MSCT Strategic Approach)," 23 September 2016. [Online]. Available: https://atarc.org/project/mobile-services-roadmap-msct-strategic-approach/.

[77] National Information Assurance Partnership (NIAP), "NIAP U.S. Government Approved Protection Profile Extended Package for Mobile Device Management Agents Version 3.0," 21 November 2016. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=403&id=403.

[78] National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile Protection Profile for Mobile Device Fundamentals Version 3.1," 16 June 2017. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm.

[79] National Information Assurance Partnership (NIAP), "U.S. Government Approved Protection Profile Protection Profile for Mobile Device Management Version 3.0," 21 November 2016. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?PPID=392&id=392.

[80] United States Office of Management and Budget (OMB), "Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services," 4 August 2016. [Online]. Available: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_20.pdf.

[81] National Institute of Standards and Technology (NIST), "United States Government Configuration Baseline (In Development)," [Online]. Available: https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline.

[82] Department of Homeland Security (DHS), "DHS Study on Mobile Device Security," April 2017. [Online]. Available: https://www.dhs.gov/publication/csd-mobile-device-security-study.

[83]	Android, "Android zero-touch enrollment," [Online]. Available: https://www.android.com/enterprise/management/zero-touch/.
[84]	Google, "Android's enterprise requirements," [Online]. Available: https://support.google.com/work/android/answer/6174145?hl=en.
[85]	Apple, "Business Support," [Online]. Available: https://support.apple.com/business.
[86]	Apple, "Configuration Profile," 3 May 2019. [Online]. Available: https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf.
[87]	Samsung, "Knox Mobile Enrollment," [Online]. Available: https://www.samsungknox.com/en/solutions/it-solutions/knox-mobile-enrollment.
[88]	Samsung, "Secured by Knox," [Online]. Available: https://www.samsungknox.com/en/secured-by-knox.
[89]	Samsung, "Devices built on Knox," [Online]. Available: https://www.samsungknox.com/en/knox-platform/supported-devices.
[90]	Samsung, "Knox features on Android," [Online]. Available: https://www.samsungknox.com/en/knox-features/android/kme.
[91]	The MITRE Corporation, "ATT&CK," [Online]. Available: https://attack.mitre.org/.
[92]	National Institute of Standards and Technology (NIST), "National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) 8144 (Draft), Assessing Threats to Mobile Devices & Infrastructure: the Mobile Threat Catalogue," [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8144/draft.
[93]	The MITRE Corporation, "ATT&CK for Mobile," [Online]. Available: https://attack.mitre.org/resources/mobile-introduction/.
[94]	The MITRE Corporation, "Common Vulnerabilities and Exposures (CVEs)," [Online]. Available: http://cve.mitre.org/.
[95]	FedRAMP, "FedRAMP Home Page," [Online]. Available: https://www.fedramp.gov/.
[96]	National Institute of Standards and Technology (NIST), "NIST Information Technlogy Laboratory National Vulnerability Database," [Online]. Available: https://nvd.nist.gov/.
[97]	Android Open Source Project, "Pixel / Nexus Security Bulletins," [Online]. Available: https://source.android.com/security/bulletin/pixel/.
[98]	Apple Computers, "Apple Security Updates," [Online]. Available: https://support.apple.com/en-us/HT201222.
[99]	Apple, "Managing Devices & Corporate Data on iOS," July 2018. [Online]. Available: https://www.apple.com/business/resources/docs/Managing_Devices_and_Corporate_Data_oniOS.pdf.
[100]	Samsung, "Android Security Updates," [Online]. Available: https://security.samsungmobile.com/securityUpdate.smsb.

ZAŁĄCZNIK D NORMY I WYTYCZNE

- National Institute of Standards and Technology (NIST) *Cybersecurity Framework Version 1.1* [5]
- NIST *Mobile Threat Catalogue* [9]
- NIST *Risk Management Framework* [8]
- NIST Special Publication (SP) 1800-4, *Mobile Device Security: Cloud and Hybrid Builds* [14]
- NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [12]
- NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations* [17]
- NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* [34]
- NIST SP 800-52 Revision 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations [37]
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [11]
- NIST SP 800-63, *Digital Identity Guidelines* [66]
- NIST SP 800-113, *Guide to SSL VPNs* [49]
- NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security* [67]
- NIST SP 800-124 Revision 2 Draft, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [13]
- NIST SP 800-163 Revision 1, *Vetting the Security of Mobile Applications* [50]
- NIST SP 800-171 Revision 2, *Protecting Controlled Unclassified Information in Non-federal Systems and Organizations* [60]

- NIST SP 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [7]
- Center for Internet Security [46]
- Executive Office of the President, Bring Your Own Device Toolkit [68]
- Federal Chief Information Officers (CIO) Council and Department of Homeland Security (DHS) Mobile Security Reference Architecture, Version 1.0 [69]
- Digital Services Advisory Group and Federal Chief Information Officers Council, Government Use of Mobile Technology Barriers, Opportunities, and Gap Analysis [70]
- International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27001:2013, *Information technology-Security techniques-Information security management systems-Requirements* [45]
- Mobile Computing Decision Example Case Study [71]
- Mobile Services Category Team (MSCT) Advanced Technology Academic Research Center (ATARC), Mobility Strategy Development Guidelines Working Group Document [72]
- MSCT ATARC, Mobile Threat Protection App Vetting and App Security Working Group Document [73]
- MSCT, Device Procurement and Management Guidance [74]
- MSCT, Mobile Device Management (MDM), MDM Working Group Document [75]
- MSCT, Mobile Services Roadmap, MSCT Strategic Approach [76]
- NIAP U.S. Government Approved Protection Profile—Extended Package for Mobile Device Management Agents Version 3.0 [77]
- NIAP U.S. Government Approved Protection Profile—Protection Profile for Mobile Device Fundamentals Version 3.1 [78]
- NIAP U.S. Government Approved Protection Profile—Protection Profile for Mobile Device Management Version 3.0 [79]

- NIAP Product Compliant List [28]
- United States Office of Management and Budget (OMB), Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services [80]
- The United States Government Configuration Baseline (USGCB) [81]
- United State Department of Homeland Security (DHS) Study on Mobile Device Security [82]

ZAŁĄCZNIK E REJESTRACJA URZĄDZEŃ MOBILNYCH Z SYSTEMAMI ANDROID, APPLE I SAMSUNG KNOX

W przypadku wdrażania wielu urządzeń mobilnych istnieje możliwość ich rejestracji i zarządzania nimi. Niektóre ustawienia mogą być fabrycznie skonfigurowane, a urządzenia mogą być dostarczane wstępnie skonfigurowane pod kątem zarządzania przez przedsiębiorstwo. Urządzenia z systemami iOS, Android i Samsung Knox mogą być bezpośrednio zintegrowane z rozwiązaniami do zarządzania mobilnością w przedsiębiorstwie (EMM), umożliwiając zarządzanie zabezpieczeniami na poziomie organizacji w oparciu o zdefiniowane zasady.

E.1 URZĄDZENIA Z SYSTEMEM ANDROID

W przypadku urządzeń z systemem Android rejestracja bezdotykowa (ang. *zero-touch*) stanowi alternatywę dla ręcznego konfigurowania takich urządzeń. Urządzenia z systemem Android są wyposażone w środki bezpieczeństwa, które system EMM może wykorzystać w ramach wdrożeń w przedsiębiorstwach. Program Android Enterprise firmy Google jest dostępny na urządzeniach z systemem Android w wersji 5.0 (Lollipop) lub nowszej. System EMM wdraża kontroler zasad jako część swojego agenta na urządzeniu. Kontroluje on lokalne zasady dotyczące urządzeń i aplikacje systemowe na urządzeniach. Platforma Android Enterprise obsługuje scenariusze COPE i BYOD poprzez rozwiązania zarządzające całym urządzeniem lub tylko profilem służbowym [83], [84].

E.2 URZĄDZENIA Z SYSTEMEM IOS

W przypadku urządzeń z systemem iOS aplikacja Apple Configurator obsługuje scenariusze *Volume Purchase* i *Device Enrollment Program*. Apple Business Manager jest rozwiązaniem do zarządzania urządzeniami mobilnymi, które umożliwia organizacjom wdrażanie urządzeń z systemem iOS. Są one zarządzane za pomocą profili konfiguracji. Profile konfiguracji mogą wymuszać stosowanie zasad bezpieczeństwa, takich jak korzystanie z wirtualnej sieci prywatnej, obsługa protokołu Kerberos w przedsiębiorstwie i dostęp do usług w chmurze. System iOS zawiera ponadto zestaw dodatkowych zabezpieczeń w tak zwanym trybie nadzorowanym, który jest stosowany na urządzeniach należących do firmy.

Zazwyczaj w przypadku wdrażania urządzeń z systemem iOS na dużą skalę w trybie nadzorowanym organizacje decydują się na korzystanie z usługi Device Enrollment Program ze względu na oszczędność pracy związanej z ręcznym konfigurowaniem każdego urządzenia. Jednak ze względu na niewielką liczbę urządzeń w naszym projekcie referencyjnym, skonfigurowaliśmy tryb nadzorowany za pomocą narzędzia Apple Configurator 2. Bardziej szczegółowy opis możliwości systemu iOS można znaleźć w przewodniku po zabezpieczeniach systemu iOS [85], [86].

E.3 URZĄDZENIA Z SYSTEMEM SAMSUNG KNOX

Rozwiązanie Samsung Knox Mobile Enrollment umożliwia dodawanie urządzeń Samsung w przedsiębiorstwie bez konieczności ręcznego rejestrowania każdego z nich. Rozwiązanie Samsung Knox Mobile Enrollment działa na urządzeniach Samsung Galaxy z systemem Android Lollipop lub nowszym. Umożliwia zdalną aprowizację urządzeń, gdy łączą się one z siecią Wi-Fi lub komórkową. Rozwiązanie Samsung Knox Mobile Enrollment współpracuje z wieloma systemami EMM, w tym z opcjami opartymi na chmurze [87], [88], [89], [90].

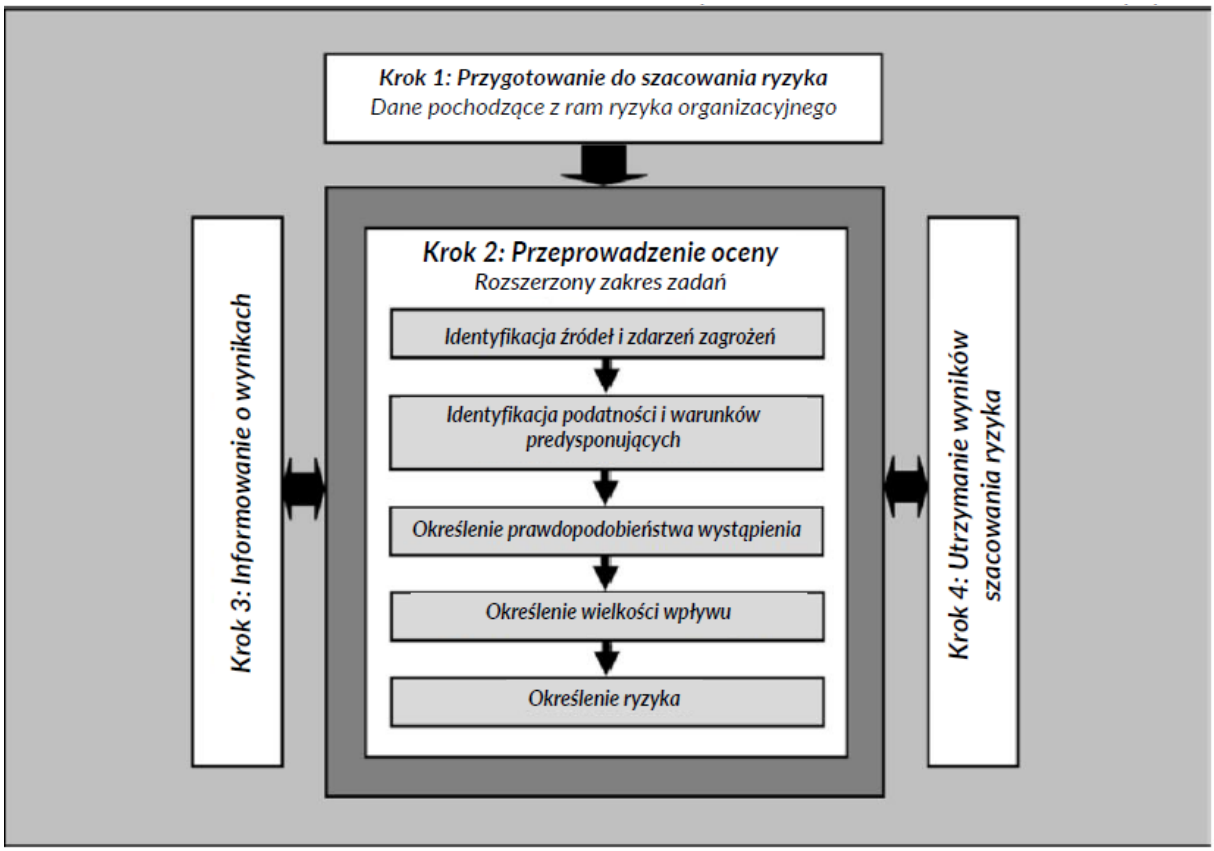
ZAŁĄCZNIK F SZACOWANIE RYZYKA

F.1 SZACOWANIE RYZYKA

W publikacji specjalnej (SP) Narodowego Instytutu Standaryzacji i Technologii (NIST) NIST SP 800-30 w wersji 1, *Guide for Conducting Risk Assessments* [12], stwierdza się, że ryzyko jest „miarą stopnia, w jakim podmiot jest zagrożony przez potencjalne okoliczności lub zdarzenia, i zazwyczaj jest funkcją: (I) niekorzystnych skutków, które powstałyby w przypadku wystąpienia okoliczności lub zdarzenia oraz (II) prawdopodobieństwa ich wystąpienia". W dalszej części przewodnik definiuje szacowanie ryzyka jako „proces identyfikacji, szacowania i nadawania priorytetu zagrożeniom dla działalności organizacji (w tym misji, funkcji, wizerunku, reputacji), aktywów organizacji, osób fizycznych, innych organizacji i państwa, wynikających z działania systemu informacyjnego. Część dotycząca zarządzania ryzykiem obejmuje analizy zagrożeń i podatności na zagrożenia oraz uwzględnia środki zaradcze w postaci planowanych lub wprowadzonych zabezpieczeń".

NCCoE zaleca, aby wszelkie dyskusje na temat zarządzania ryzykiem, szczególnie na poziomie przedsiębiorstwa, rozpoczynały się od kompleksowego zapoznania się z publikacją NIST SP 800-37 w wersji 2, *Risk Management Framework for Information Systems and Organizations* – materiałem, który jest dostępny publicznie. Wytyczne dotyczące ram zarządzania ryzykiem (*ang. Risk Management Framework – RMF*), jako całość, okazały się nieocenione, dając nam punkt odniesienia do oszacowania ryzyka, na podstawie którego opracowaliśmy projekt, charakterystykę bezpieczeństwa rozwiązania i niniejszy przewodnik.

Niniejszy punkt zawiera szczegółowe informacje na temat szacowania ryzyka podjętego w celu poprawy stanu bezpieczeństwa mobilnego fikcyjnej organizacji Orvilia Development. Zazwyczaj szacowanie ryzyka oparte na publikacji NIST SP 800-30 w wersji 1 przebiega zgodnie z czteroetapowym procesem przedstawionym na rysunku F-1: Przygotowanie do oceny, przeprowadzenie oceny, informowanie o wynikach i utrzymanie oceny.



Rysunek F-1 Proces szacowania ryzyka

Aby zapewnić jak największą wartość tego działania:

- Skupiliśmy się na przygotowaniach, w ramach których ustaliliśmy kontekst oceny ryzyka.
- Przeprowadziliśmy szacowanie ryzyka, w wyniku którego powstała lista zagrożeń dla bezpieczeństwa informacji, które zostały uszeregowane według poziomu ryzyka i wykorzystane do podjęcia decyzji dotyczących reakcji na ryzyko.
- Postępowaliśmy zgodnie z procesem opisanym w rozdziale 3 publikacji NIST SP 800-30 w wersji 1 [12], aby przeprowadzić szacowanie ryzyka związanego z obecną infrastrukturą mobilną.

Zalecamy, aby organizacje przeprowadzające szacowanie ryzyka informowały o jego wynikach i przeprowadzały jego aktualizację, ale działania te zostały uznane za wykraczające poza zakres tego projektu. W ramach procesu szacowania wykonano zadania opisane poniżej.

F.1.1 Zadanie 1-1: Cel szacowania ryzyka

Określenie celu szacowania ryzyka dotyczącego informacji, które ma ono dostarczyć, oraz decyzji, które ma wspierać.

Celem szacowania ryzyka w organizacji Orvilia Development było zidentyfikowanie i udokumentowanie nowych zagrożeń dla jej misji wynikających z dodania programu mobilności.

Wyniki szacowania ryzyka wpłynęły na następujące decyzje dotyczące wdrożenia urządzeń mobilnych w organizacji Orvilia:

- wdrożenie nowych mechanizmów bezpieczeństwa;
- zmiany w konfiguracji istniejącej infrastruktury;
- aktualizacje zasad bezpieczeństwa i właściwego użytkowania związanych z programem mobilności organizacji.

F.1.2 Zadanie 1-2: Zakres szacowania ryzyka

Określenie zakresu szacowania ryzyka pod kątem możliwości zastosowania w organizacji, ram czasowych oraz kwestii dotyczących architektury/technologii.

Możliwość zastosowania w organizacji:

Zakres niniejszego szacowania ryzyka był ograniczony do systemów, na które miało wpływ wdrożenie programu mobilności. Nie obejmowało ono istniejącej infrastruktury IT, na którą nie przewidywano żadnego wpływu. W ramach swojej pierwotnej architektury firma Orvilia wdrożyła urządzenia będące jej własnością, z których pracownicy mogą korzystać również prywatnie (COPE). Pracownicy firmy Orvilia wykorzystywali urządzenia mobilne do lokalnej i zdalnej pracy oraz ograniczonej aktywności osobistej (np. rozmów telefonicznych, przesyłania wiadomości, korzystania z aplikacji społecznościowych i obsługi prywatnych wiadomości e-mail).

W związku z nowym kontraktem rządowym firmy Orvilia, w ramach szacowania ryzyka oceniono również jej wdrożenie urządzeń mobilnych pod kątem możliwości uzyskiwania

dostępu do danych rządowych i ich przechowywania, przy jednoczesnym spełnieniu obowiązujących wymogów w zakresie bezpieczeństwa informacji i prywatności.

Chociaż nie jest to bezpośrednio związane z szacowaniem ryzyka, firma Orvilia będzie musiała wykazać zgodność z rządowymi standardami i politykami ustanowionymi w celu poprawy bezpieczeństwa danych. W związku z tym musiała ona określić, w jaki sposób dostosować swoją strategię identyfikacji, ochrony, wykrywania, reagowania i usuwania skutków zagrożeń związanych z jej programem mobilności do rządowej polityki i standardów.

Ramy czasowe:

Ponieważ było to pierwsze szacowanie ryzyka przeprowadzone przez organizację Orvilia, proces ten był bardziej czasochłonny niż w przypadku przyszłych cykli zarządzania ryzykiem. Orvilia ukończyła pierwsze szacowanie ryzyka w ciągu sześciu miesięcy.

Kwestie dotyczące architektury/technologii:

Niniejsza ocena ryzyka obejmowała mobilne wdrożenie w Orvilia, na które składają się urządzenia mobilne używane do uzyskiwania dostępu do zasobów przedsiębiorstwa wraz z wszelkimi komponentami zaplecza IT używanymi do zarządzania tymi urządzeniami mobilnymi lub zapewniania im określonych usług.

Poniżej przedstawiono przegląd mobilnych komponentów wdrożenia w oryginalnej (obecnej) architekturze organizacji Orvilia.

- **Urządzenie mobilne:** Urządzenie mobilne to niewielkie urządzenie z rozbudowanym systemem operacyjnym, co najmniej jednym interfejsem sieci bezprzewodowej i możliwością obsługi aplikacji. Funkcje te są uważane za niezbędne, aby organizacja Orvilia miała mobilny i efektywny dostęp do danych przedsiębiorstwa.
- **Sieci komunikacyjne i transmisja danych:** Urządzenia mobilne będą nawiązywać połączenie z Internetem za pomocą swoich adapterów sieci komórkowej lub Wi-Fi. Ponieważ połączenia mogą być nawiązywane z niezabezpieczonymi punktami dostępu lub mogą przechodzić przez niezaufane sieci, należy wziąć pod uwagę

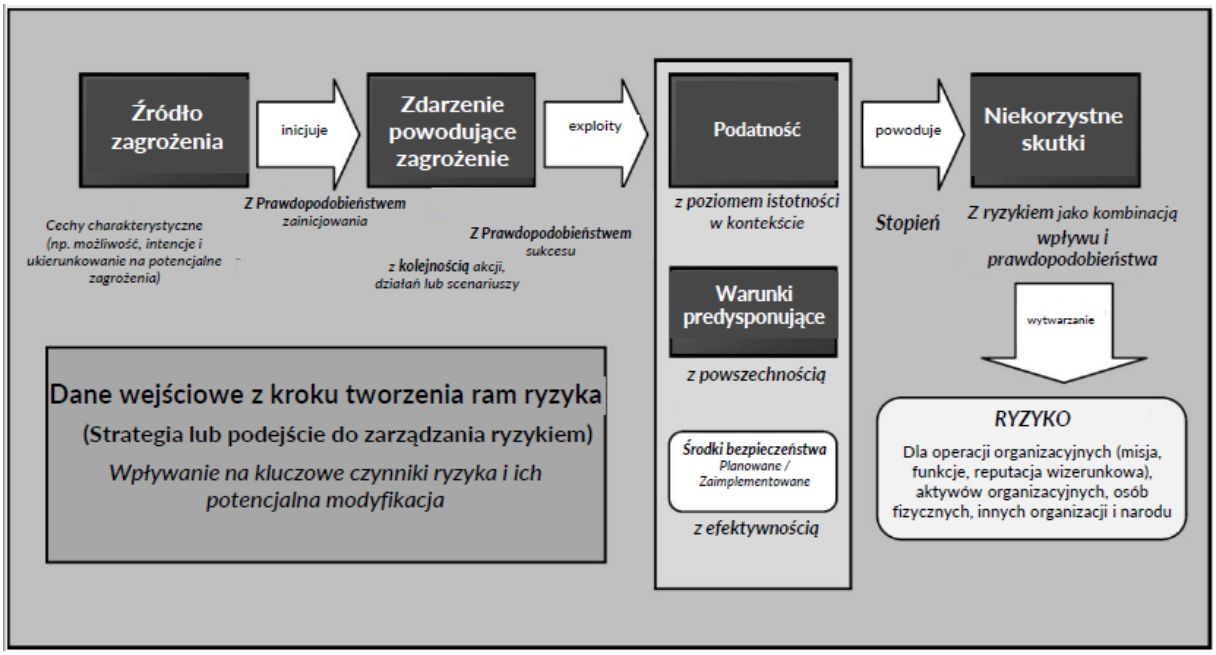
ryzyko związane z bezpieczeństwem tych połączeń i przesyłanych przez nie danych. Ponadto organizacja będzie musiała rozważyć ryzyko wynikające z zezwolenia na połączenia przychodzące z urządzeń mobilnych przez Internet.

- **Publiczne sklepy z aplikacjami:** W przypadku strategii wdrażania COPE pracownicy mają możliwość pobrania dowolnej aplikacji mobilnej dostępnej w oficjalnych sklepach z aplikacjami (np. Google Play Store). Platformy te analizują aplikacje pod kątem złośliwego zachowania, jednak nadal możliwe jest, że nie spełniają one potrzeb firmy Orvilia w zakresie prywatności użytkowników albo stanowią zagrożenie dla urządzeń lub danych. W związku z tym ryzyko związane z takimi aplikacjami powinno zostać uwzględnione w tej ocenie.
- **Infrastruktura dostawców urządzeń i systemów operacyjnych:** Elementy sprzętowe, oprogramowanie zwykłe i układowe, które składają się na każdy model urządzenia mobilnego, mogą się różnić, szczególnie w przypadku urządzeń pochodzących od różnych producentów i sprzedawców, którzy mogą wykorzystywać technologie stosowane wyłącznie w ich produktach. Ważne będzie wybranie urządzeń, które charakteryzują się mechanizmami bezpieczeństwa zgodnymi ze strategią ograniczania ryzyka organizacji. Jednak ryzyko specyficzne dla danych komponentów urządzenia (np. mikroukładów lub wersji sterowników) nie będzie objęte zakresem tej oceny.
- **Systemy przedsiębiorstwa:** Jeśli urządzenie mobilne będące przedmiotem potencjalnego ataku może połączyć się z przedsiębiorstwem, stwarza bezpośrednie zagrożenie dla wszelkich systemów i danych, do których może uzyskać dostęp. Takie systemy będą obejmować lokalne sklepy z aplikacjami mobilnymi, technologie zarządzania urządzeniami mobilnymi, serwery poczty elektronicznej, serwery plików i intranetowe serwery sieci Web. Naruszenie bezpieczeństwa któregokolwiek z tych systemów może mieć wpływ na inne systemy, do których urządzenie mobilne nie ma bezpośredniego dostępu. Zagrożenia dla wszystkich takich systemów ze strony urządzeń mobilnych powinny zostać uwzględnione w tej ocenie.

F.1.3 Zadanie 1-3: Założenia i ograniczenia szacowania ryzyka

Określenie konkretnych założeń i ograniczeń, zgodnie z którymi przeprowadzane jest szacowanie ryzyka.

Założenia i ograniczenia szacowania ryzyka zostały opracowane przy użyciu ogólnego modelu ryzyka z publikacji NIST SP 800-30 w wersji 1, jak pokazano na rysunku F-2.



Rysunek F-2 Ogólny model ryzyka z publikacji NIST 800-30

F.1.3.1 Założenia szacowania ryzyka

Niektóre zagrożenia oraz wynikające z nich ryzyko i skutki obejmują kilka poziomów. W przypadkach, w których te zagrożenia i skutki mają kilka możliwych poziomów, założono, że firma Orvilia udokumentuje je przy użyciu koncepcji najwyższej wartości. Założenie dotyczące największego ryzyka stanowiło następnie podstawę działań ograniczających ryzyko. Na przykład, gdy ryzyko związane z zagrożeniem mogło mieć umiarkowane, poważne lub bardzo poważne skutki, wybrano bardzo poważne skutki, a te bardzo poważne zagrożenia zostały potraktowane priorytetowo w celu ich złagodzenia.

F.1.3.2 Ograniczenia szacowania ryzyka

Informacje dotyczące poniższych elementów zostały wykorzystane jako dane wejściowe dla ograniczeń szacowania ryzyka:

- źródła zagrożeń
- zdarzenia powodujące zagrożenie
- podatności i warunki predysponujące
- prawdopodobieństwo
- skutki
- podejścia do szacowania i analizy ryzyka
- zasoby dostępne na potrzeby szacowania
- umiejętności i wiedza specjalistyczna

Źródła zagrożeń

Kierownictwo i menedżerowie firmy Orvilia jako potencjalne zagrożenia zidentyfikowali dwa źródła zagrożeń. Personel techniczny otrzymał zestawienia środków bezpieczeństwa zawarte w tym przewodniku, aby pokazać pracownikom, jak zwiększy się poziom bezpieczeństwa po wdrożeniu w firmie Orvilia przykładowego rozwiązania.

Ponadto, ze względu na zakres szacowania ryzyka ukierunkowany na cyberbezpieczeństwo, nie uwzględniono innych źródeł zagrożeń (np. niezamierzonych zagrożeń związanych ze sprzętem, oprogramowaniem lub wadami projektu i architektury systemu).

Jak wskazano w punkcie F.1.6, Zadanie 2-1: Identyfikacja i charakterystyka źródeł zagrożeń, w ramach szacowania ryzyka zidentyfikowano następujące źródła zagrożeń:

- konkurencja firmy Orvilia
- podmioty na szczeblu krajowym

Zdarzenia powodujące zagrożenie

- Zdarzenia powodujące zagrożenia zostały opisane, zarówno szczegółowo, jak i ogólnie w ramach szacowania ryzyka. Podobne zdarzenia powodujące zagrożenia zostały połączone w jedno, obszerniejsze zagrożenie.

- Uwzględniono tylko te zdarzenia powodujące zagrożenia, które zostały wcześniej zaobserwowane przez wiarygodne źródło (np. zgłoszone jako już zaistniałe przez inne organizacje), opierając się głównie na katalogu zagrożeń mobilnych NIST, *National Cybersecurity Center of Excellence* [9].
- Zdarzenia powodujące zagrożenia polegające na wykorzystaniu podatności sieci komórkowej, w tym pasma podstawowego telefonii komórkowej, w uzasadniony sposób przekraczały możliwości firmy Orvilia w zakresie ich bezpośredniej identyfikacji i przeciwdziałania im, dlatego nie zostały poddane dalszej ocenie.
- Zdarzenia powodujące zagrożenia polegające na wykorzystaniu podatności w sprzęcie niskiego poziomu, oprogramowaniu układowym i sterownikach urządzeń w uzasadniony sposób przekraczały możliwości firmy Orvilia w zakresie ich bezpośredniej identyfikacji i przeciwdziałania im, dlatego nie zostały poddane dalszej ocenie.
- Zdarzenia powodujące zagrożenia polegające na wykorzystaniu podatności w łańcuchu dostaw w uzasadniony sposób przekraczały możliwości firmy Orvilia w zakresie ich bezpośredniej identyfikacji i przeciwdziałania im, dlatego nie zostały poddane dalszej ocenie.

Podatności i warunki predysponujące

- Podatności urządzeń mobilnych uwzględnione podczas szacowania ryzyka obejmowały podatności w mobilnych systemach operacyjnych i aplikacjach mobilnych, w tym w bibliotekach oprogramowania innych firm.
- Wzięto pod uwagę podatności w powszechnie używanych protokołach sieci innych niż komórkowe, takich jak Bluetooth i Wi-Fi.
- Uwzględniono podatności związane z potencjalnym systemem zarządzania mobilnością w przedsiębiorstwie (EMM).
- Pozyskano dodatkowe informacje i dokonano ustaleń na podstawie załącznika F do publikacji NIST SP 800-30 w wersji 1.

Prawdopodobieństwo

- Prawdopodobieństwo zostało określone na podstawie załącznika G do publikacji NIST SP 800-30 w wersji 1.

Uwaga: Ocena ogólnego prawdopodobieństwa jest obliczana na podstawie prawdopodobieństwa zainicjowania i prawdopodobieństwa, że zdarzenie powodujące zagrożenie będzie miało niekorzystny wpływ, przy użyciu tabeli G-5 w załączniku G publikacji NIST SP 800-30 w wersji 1 [12]. Oceny dwóch ostatnich zmiennych opierały się w dużej mierze na subiektywnej ocenie pracowników firmy Orvilia.

Skutki

- Skutki określono na podstawie załącznika H do publikacji NIST SP 800-30 w wersji 1.

Uwaga: Oceny skutków opierały się w dużej mierze na subiektywnej ocenie pracowników firmy Orvilia.

Podejścia do szacowania i analizy ryzyka

- Szacowanie ryzyka koncentrowało się na zidentyfikowaniu wstępnego zestawu zagrożeń dla wdrożenia urządzeń mobilnych w firmie Orvilia.
- Podejścia do opisywania zagrożeń i ich skutków zostały oparte na modelu ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) [91].
- Ocena ryzyka została określona na podstawie zarówno ogólnego prawdopodobieństwa, jak i poziomu wpływu przy użyciu tabeli I2 w załączniku i do publikacji NIST 800-30 w wersji 1 [12].

Zasoby dostępne na potrzeby szacowania

- Firma Orvilia zadbała o to, aby odpowiedni personel posiadający wymaganą wiedzę specjalistyczną był dostępny do przeprowadzenia oceny w wyznaczonym czasie.
- Zapewniła również finansowanie dla personelu zajmującego się analizą ryzyka.
- Pracownicy firmy Orvilia, którzy przeprowadzili szacowanie ryzyka, dysponowali niezbędnymi systemami IT i oprogramowaniem.

Umiejętności i wiedza specjalistyczna

- Szacowanie ryzyka zostało przeprowadzone przez ekspertów wykorzystujących najlepsze praktyki branżowe i ramy szacowania ryzyka NIST.

F.1.4 Zadanie 1-4: Źródła informacji o zagrożeniach, podatnościach i wpływie na potrzeby szacowania ryzyka

Określenie źródeł opisowych informacji o zagrożeniach, podatnościach i skutkach, które zostaną wykorzystane w szacowaniu ryzyka.

Firma Orvilia wykorzystała następujące metody do identyfikacji zagrożeń, podatności i skutków wdrożenia infrastruktury mobilnej.

F.1.4.1 Źródła informacji o zagrożeniach

W ramach tego szacowania ryzyka za wiarygodne źródła informacji o zagrożeniach uznano katalog zagrożeń dla urządzeń mobilnych (MTC) NIST [9] wraz z powiązanym z nim raportem międzyresortowym NIST IR 8144, *Assessing Threats to Mobile Devices & Infrastructure* [92] oraz profil mobilny ATT&CK organizacji MITRE [93]. Każdy wpis w katalogu MTC zawiera kilka informacji: identyfikator, kategorię, ogólny opis, szczegółowe informacje na temat pochodzenia, przykłady wykorzystania w atakach, przykłady ze słownika CVP [94] możliwe środki zaradcze i źródła akademickie.

ATT&CK organizacji MITRE to rozbudowana baza wiedzy i model zachowań cyberprzestępców. w bazie ATT&CK szczegółowo opisano konkretne techniki, które mogą być wykorzystywane przez cyberprzestępców. Każdy wpis dotyczący techniki zawiera zazwyczaj szczegółowy opis techniczny, środki zaradcze, analizę wykrywania, przykłady wykorzystania przez złośliwe podmioty i odniesienia. Model ATT&CK organizuje te techniki w wysokopoziomowe cele taktyczne złośliwych podmiotów, zwane taktykami. Podstawowym zastosowaniem bazy ATT&CK jest jej wykorzystanie przez organizacje do oceny stanu ich cyberbezpieczeństwa i ustalania priorytetów w zakresie wdrażania zdolności obronnych. W profilu mobilnym ATT&CK opisano taktyki i techniki specyficzne dla środowiska mobilnego.

Ze względu na fakt, że firma Orvilia korzysta obecnie z usług w chmurze, określono wyniki federalnego programu zarządzania ryzykiem i autoryzacją [95] oraz powiązane

środki bezpieczeństwa z publikacji NIST SP 800-53 jako wchodzące w zakres szacowania ryzyka.

F.1.4.2 Źródła informacji o podatnościach

Podatności są zazwyczaj związane z mobilnymi systemami operacyjnymi, sterownikami urządzeń, aplikacjami mobilnymi i bibliotekami innych firm. Mogą jednak występować na każdym poziomie technologii mobilnych. W celu uzyskania aktualnych informacji dotyczących podatności na zagrożenia, w niniejszym szacowaniu ryzyka za wiarygodne źródło danych uznano krajową bazę danych o podatnościach na zagrożenia (*ang. National Vulnerability Database – NVD*) [96]. NVD to oparte na standardach rządowe repozytorium danych dotyczących zarządzania podatnościami. Informacje z NVD zostały uzupełnione o przeglądy ujawnionych podatności od poszczególnych producentów, takich jak te opublikowane w biuletynach bezpieczeństwa Pixel/Nexus [97] dla systemu Android, aktualizacjach zabezpieczeń Apple [98] dla systemu iOS, publikacji *Managing Devices & Corporate Data* dla systemu iOS [99] oraz aktualizacjach zabezpieczeń systemu Android [100] dla urządzeń Samsung z tym systemem.

F.1.4.3 Źródła informacji o skutkach

W ramach szacowania ryzyka jako główne źródło informacji na temat określania skutków wybrano scenariusz opisany w punkcie F.1.2. W scenariuszu tym jako krytyczne dla misji organizacji wskazano następujące systemy:

- domenę Microsoft Active Directory
- serwer poczty elektronicznej Microsoft Exchange
- aplikację internetową do rejestracji czasu pracy
- aplikację internetową do obsługi podróży
- firmowe urządzenia mobilne

Przykładem udanego ataku na urządzenie mobilne jest próba pozyskania danych uwierzytelniających do aplikacji internetowej do obsługi podróży i wykorzystania ich

do penetracji serwera aplikacji. Chociaż firma Orvilia mogłaby zaakceptować minimalny czas niedostępności aplikacji internetowej, atakujący mógłby wykorzystać swoją pozycję do zdobycia przyczółka w infrastrukturze Orvilia, aby przejść do bardziej krytycznych systemów w środowisku, takich jak serwer poczty elektronicznej. Naruszenie bezpieczeństwa serwera poczty elektronicznej miałoby poważne skutki, mogące doprowadzić do poważnych szkód w organizacji.

F.1.5 Zadanie 1-5: Określenie modelu ryzyka i podejścia analitycznego na potrzeby szacowania ryzyka

Określenie modelu ryzyka i podejścia analitycznego, które zostaną wykorzystane w szacowaniu ryzyka.

W ramach szacowania ryzyka w podejściu analitycznym wykorzystano jakościowe (tj. subiektywne) oceny ryzyka (tj. bardzo niskie, niskie, umiarkowane, wysokie i bardzo wysokie). Podejście było przede wszystkim skoncentrowane na zagrożeniach, jak opisano w punkcie F.1.6.

F.1.6 Zadanie 2-1: Identyfikacja i charakterystyka głównych źródeł zagrożeń

Identyfikacja i charakterystyka głównych źródeł zagrożeń, w tym charakterystyki pod kątem zdolności, zamiaru i ukierunkowania w przypadku zagrożeń ze strony przeciwników oraz zakresu skutków w przypadku zagrożeń niezwiązanych z przeciwnikami.

Firma Orvilia przeanalizowała tabelę D-2 z publikacji NIST SP 800-30 w wersji 1: „Taksonomia źródeł zagrożeń” [12] i zidentyfikowała następujące źródła zagrożeń:

Tabela F-1 Główne źródła zagrożeń

Identyfikator	Źródło zagrożenia	Opis	Charakterystyka
TS-1	Adwersarz, organizacja, konkurencja	Konkurenci firmy Orvilia starają się wykorzystać jej zależność od zasobów cyfrowych, w szczególności danych powierzonych przez klientów, w celu zwiększenia swojego udziału w rynku.	Zdolność, zamiar, ukierunkowanie
TS-2	Adwersarz, państwo	Podmioty na poziomie krajowym wykradające wrażliwe dane rządowe z niezabezpieczonych urządzeń i infrastruktury.	Zdolność, zamiar, ukierunkowanie

Orvilia stworzyła poniższą tabelę jako wynik zadania 2-1, aby zapewnić odpowiednie dane wejściowe dla tabel ryzyka. Określono w niej źródła zagrożeń zidentyfikowane w publikacji NIST SP 800-30 w wersji 1 wraz z powiązaną oceną ryzyka w zakresie zdolności, zamiaru i ukierunkowania (przy użyciu wspomnianej wcześniej pięciostopniowej skali: bardzo niskie, niskie, umiarkowane, wysokie i bardzo wysokie).

Ocena firmy Orvilia wykazała, że wszystkie zdarzenia powodujące zagrożenie mogą być inicjowane przez oba źródła zagrożeń (organizację/konkurencję i podmiot państwa narodowego).

Zdolność odnosi się do poziomu specjalistycznej wiedzy złośliwego podmiotu. Zamiar odnosi się do celu złośliwego podmiotu. Ukierunkowanie odnosi się do metod rozpoznania i selekcji stosowanych przez złośliwy podmiot.

Tabela F-2 Skala jakościowa źródeł zagrożeń

Identyfikator	Zdarzenia powodujące zagrożenie istotne dla źródeł zagrożeń	W zakresie	Zdolność	Zamiar	Ukierunkowanie
TS-1	Wszystkie zdarzenia powodujące zagrożenia (zdarzenia powodujące zagrożenia 1–12)	**Tak**	**Wysokie**	**Wysokie**	**Wysokie**
TS-2	Wszystkie zdarzenia powodujące zagrożenia (zdarzenia powodujące zagrożenia 1–12)	**Tak**	**Bardzo wysokie**	**Bardzo wysokie**	**Bardzo wysokie**

F.1.7 Zadanie 2-2: Identyfikacja potencjalnych zdarzeń powodujących zagrożenie

Identyfikacja potencjalnych zdarzeń powodujących zagrożenie, ich znaczenia oraz źródeł zagrożeń, które mogą je zainicjować.

Zdarzenia powodujące zagrożenie wykorzystane w przykładowym rozwiązaniu opisano poniżej. W ramach zdarzeń tych opisano, w jaki sposób bezpieczeństwo urządzeń mobilnych firmy Orvilia może zostać naruszone w wyniku złośliwych działań. Wszystkie zdarzenia powodujące zagrożenie są powiązane z obydwoma źródłami zagrożeń zidentyfikowanymi w punkcie F.1.6.

Firma Orvilia przeanalizowała przykładowe tabele w publikacji NIST SP 800-30 w wersji 1 – tabele E-1, E-2, E-3, E-4 i E-5 – oraz źródła zagrożeń mobilnych zidentyfikowane w zadaniu 1-4. Stosując ten proces, kierownictwo firmy Orvilia zidentyfikowało zdarzenia powodujące zagrożenie opisane poniżej.

F.1.7.1 Zdarzenie powodujące zagrożenie 1 (TE-1) — Nieautoryzowany dostęp do wrażliwych informacji za pośrednictwem złośliwej lub naruszającej prywatność aplikacji

Aplikacja mobilna może służyć do prób gromadzenia i eksfiltracji wszelkich danych, do których uzyskała dostęp. Obejmuje to wszelkie informacje generowane podczas korzystania z aplikacji (np. dane wejściowe wprowadzane przez użytkownika), przyznane przez niego uprawnienia (np. dostęp do kontaktów, kalendarza, dzienników połączeń, rolki z aparatu) oraz ogólne dane urządzenia dostępne dla dowolnej aplikacji (np. międzynarodowy identyfikator urządzenia mobilnego, marka i model urządzenia, numer seryjny). Co więcej, jeśli złośliwa aplikacja wykorzysta lukę w innych programach, systemie operacyjnym lub oprogramowaniu układowym urządzenia, aby doprowadzić do eskalacji uprawnień, może uzyskać nieautoryzowany dostęp do wszelkich danych przechowywanych na urządzeniu lub w inny sposób dostępnych za jego pośrednictwem.

F.1.7.2 Zdarzenie powodujące zagrożenie 2 — Kradzież danych uwierzytelniających za pośrednictwem kampanii wiadomości SMS lub e-mail służącej do wyłudzania informacji

Złośliwe podmioty mogą tworzyć fałszywe strony internetowe, które mają naśladować wygląd i działanie oficjalnych witryn i zachęcać użytkowników do uwierzytelnienia się na nich poprzez dystrybucję wiadomości za pośrednictwem usługi SMS lub poczty elektronicznej. Skuteczne wykorzystanie technik inżynierii społecznej, takich jak podszywanie się pod autorytet lub stwarzanie poczucia pilności, może skłonić użytkownika do rezygnacji z analizy wiadomości i przystąpienia do uwierzytelnienia na fałszywej stronie internetowej. Wprowadzone dane uwierzytelniające użytkownika są przechwytywane i przechowywane, a następnie (zazwyczaj) przekazywane do prawdziwej strony internetowej w celu rozwiania podejrzeń.

F.1.7.3 Zdarzenie powodujące zagrożenie 3 — Złośliwe aplikacje instalowane za pośrednictwem adresu URL w wiadomościach SMS lub e-mail

Złośliwe podmioty mogą wysyłać użytkownikom wiadomości SMS lub e-mail zawierające adres URL, pod którym jest hostowana złośliwa aplikacja. Zazwyczaj takie wiadomości są tworzone z wykorzystaniem technik inżynierii społecznej, które mają na celu zniechęcenie odbiorców do sprawdzenia charakteru wiadomości, zwiększając tym samym prawdopodobieństwo skorzystania z adresu URL za pomocą urządzenia mobilnego. Jeśli dojdzie do skorzystania z adresu URL, urządzenie podejmie próbę pobrania i zainstalowania aplikacji. Skuteczne wykorzystanie socjotechniki przez atakującego może skłonić nawet ostrożnego użytkownika do udzielenia wszelkiego zaufania wymaganego przez twórcę i wszystkich uprawnień wymaganych przez aplikację. Udzielenie pierwszej zgody ułatwia instalację innych złośliwych aplikacji od tego samego twórcy, a przyznanie drugiej zwiększa potencjał aplikacji do wyrządzenia bezpośrednich szkód.

F.1.7.4 Zdarzenie powodujące zagrożenie 4 — Utrata poufności i integralności w wyniku wykorzystania znanej podatności w systemie operacyjnym lub oprogramowaniu układowym

Gdy złośliwe oprogramowanie z powodzeniem wykorzystuje lukę w zabezpieczeniach mobilnego systemu operacyjnego lub sterowników urządzenia, wprowadzony kod jest zazwyczaj wykonywany z podwyższonymi uprawnieniami, a następnie wydaje polecenia z poziomu użytkownika głównego lub jądra systemu operacyjnego. Niektórym atakującym może to wystarczyć do osiągnięcia celu, ale zaawansowane złośliwe podmioty zazwyczaj próbują zainstalować dodatkowe złośliwe narzędzia i ustanowić trwałą obecność. W przypadku powodzenia atakujący będzie mógł przeprowadzić dalsze ataki na użytkownika, urządzenie lub inne systemy, z którymi łączy się urządzenie. W rezultacie wszelkie dane przechowywane na urządzeniu, generowane przez nie lub dostępne za jego pośrednictwem w tym czasie lub w przyszłości mogą zostać naruszone.

F.1.7.5 Zdarzenie powodujące zagrożenie 5 — Naruszenie prywatności poprzez niewłaściwe wykorzystanie czujników urządzenia

Złośliwe podmioty z dostępem (autoryzowanym lub nieautoryzowanym) do czujników urządzenia (mikrofonu, kamery, żyroskopu, systemu GPS i radia) mogą wykorzystywać je do prowadzenia inwigilacji. Może ona być skierowana przeciwko użytkownikowi, jak w przypadku śledzenia lokalizacji urządzenia, lub może być stosowana bardziej ogólnie, np. poprzez nagrywanie dźwięków z otoczenia. Dane przechwycone przez czujniki, takie jak nagranie spotkania kierownictwa, mogą być natychmiast użyteczne dla złośliwego podmiotu. Dane mogą być również analizowane oddzielnie lub w połączeniu z innymi danymi w celu uzyskania wrażliwych informacji. Na przykład, nagrania audio aktywności na urządzeniu lub w jego pobliżu mogą być wykorzystane do probabilistycznego określenia danych wejściowych wprowadzanych przez użytkownika na ekranach dotykowych i klawiaturach – praktycznie zmieniając urządzenie w zdalny rejestrator klawiszy.

F.1.7.6 Zdarzenie powodujące zagrożenie 6 — Naruszenie integralności urządzenia lub jego komunikacji sieciowej poprzez instalację złośliwego systemu EMM/MDM, sieci, profili VPN lub certyfikatów.

Złośliwe podmioty, które pomyślnie zainstalują na urządzeniu profil lub certyfikat systemu EMM/MDM, sieciowy lub sieci VPN, uzyskają dodatkową kontrolę nad urządzeniem lub jego komunikacją. Obecność profilu EMM/MDM umożliwi atakującemu nadużywanie istniejących interfejsów API systemu operacyjnego w celu wysyłania do urządzenia szerokiej gamy poleceń. Może to umożliwić złośliwemu podmiotowi uzyskanie informacji o urządzeniu, instalowanie lub ograniczanie aplikacji lub zdalne lokalizowanie, blokowanie lub czyszczenie urządzenia. Złośliwe profile sieciowe mogą umożliwić złośliwemu podmiotowi automatyczne zmuszanie urządzenia do łączenia się z punktami dostępu znajdującymi się pod jego kontrolą w celu przeprowadzenia ataku typu *person-in-the-middle* na wszystkie połączenia wychodzące. Alternatywnie, profile VPN mogą umożliwiać niewykrytą eksfiltrację wrażliwych danych poprzez ich szyfrowanie – ukrywa je to przed narzędziami do

skanowania sieci. Ponadto złośliwe certyfikaty mogą umożliwić złośliwemu podmiotowi zmuszenie urządzenia do automatycznego zaufania połączeniom ze złośliwymi serwerami internetowymi, bezprzewodowymi punktami dostępowymi lub instalacji aplikacji znajdujących się pod kontrolą atakującego.

F.1.7.7 Zdarzenie powodujące zagrożenie 7 — Utrata poufności wrażliwych informacji poprzez podsłuchiwanie niezaszyfrowanej komunikacji urządzenia

Złośliwe podmioty mogą z łatwością podsłuchiwać komunikację za pośrednictwem niezaszyfrowanych sieci bezprzewodowych, takich jak publiczne punkty dostępu Wi-Fi, które są powszechnie dostępne w kawiarniach i hotelach. Jeśli urządzenie jest podłączone do takiej sieci, atakujący może uzyskać nieautoryzowany dostęp do wszelkich danych wysyłanych lub odbieranych przez urządzenie dla każdej sesji, która nie jest jeszcze chroniona przez szyfrowanie w warstwie transportowej lub aplikacji. Nawet jeśli przesyłane dane zostały zaszyfrowane, osoba atakująca może mieć dostęp do domen, adresów IP i usług (oznaczonych numerami portów), z którymi łączy się urządzenie. Takie informacje mogą zostać wykorzystane w przyszłych atakach typu *watering hole* lub *person-in-the-middle* na użytkownika urządzenia. Ponadto wgląd w ruch w warstwie sieciowej umożliwia złośliwemu podmiotowi przeprowadzanie ataków bocznymi kanałami na zaszyfrowane wiadomości, co nadal może skutkować utratą poufności. Co więcej, podsłuchiwanie niezaszyfrowanych wiadomości podczas wykonywania protokołu uzgodnienia w celu ustanowienia zaszyfrowanej sesji z innym hostem lub punktem końcowym może ułatwić ataki, które ostatecznie zagrażają bezpieczeństwu sesji.

F.1.7.8 Zdarzenie powodujące zagrożenie 8 — Naruszenie integralności urządzenia poprzez zastosowanie kodu odblokowującego, który został zaobserwowany, wywnioskowany lub pozyskany na drodze ataku siłowego

Złośliwy podmiot może pozyskać kod odblokowujący urządzenie użytkownika poprzez jego bezpośrednią obserwację, atak kanałem bocznym lub atak siłowy. Aby zastosować pierwszą technikę, wystarczy zbliżyć się do urządzenia. Tylko trzecia technika wymaga fizycznego dostępu do niego. Jednak ataki bocznym kanałem,

w którym kod odblokowujący uzyskuje się poprzez wywnioskowanie go z czynności dotykania i przeciągania palcem po ekranie, mogą być podejmowane przez aplikacje z dostępem do dowolnych urządzeń peryferyjnych wykrywających dźwięk lub ruch (np. mikrofonu, żyroskopu lub akcelerometru). Po uzyskaniu kodu odblokowującego urządzenie, złośliwy podmiot z fizycznym dostępem do niego uzyska natychmiastowy wgląd we wszelkie dane lub funkcje, które nie są chronione przez dodatkowe mechanizmy kontroli dostępu. Dodatkowo, jeśli użytkownik używał kodu odblokowującego urządzenie jako danych uwierzytelniających do innych systemów, złośliwy podmiot może uzyskać do nich nieautoryzowany dostęp.

F.1.7.9 Zdarzenie powodujące zagrożenie 9 — Nieautoryzowany dostęp do usług zaplecza poprzez luki w uwierzytelnianiu lub przechowywaniu danych uwierzytelniających w wewnętrznie opracowanych aplikacjach

Jeśli złośliwy podmiot uzyska nieautoryzowany dostęp do urządzenia mobilnego, ma on również dostęp do znajdujących się na nim danych i aplikacji. Urządzenie mobilne może zawierać wewnętrzne aplikacje organizacji, które dają dostęp do wrażliwych danych lub usług zaplecza. Podatność ta może wynikać ze słabości lub luk w mechanizmach uwierzytelniania lub przechowywania danych uwierzytelniających zaimplementowanych w aplikacji wewnętrznej.

F.1.7.10 Zdarzenie powodujące zagrożenie 10 — Nieautoryzowany dostęp do zasobów przedsiębiorstwa z urządzenia niezarządzanego i narażonego na naruszenie bezpieczeństwa

Pracownik, który uzyskuje dostęp do zasobów przedsiębiorstwa z niezarządzanego urządzenia mobilnego, naraża organizację na skutki podatności, które mogą obejmować naruszenie bezpieczeństwa danych firmy. W przypadku urządzeń niezarządzanych nie są wykorzystywane mechanizmy bezpieczeństwa wdrożone przez organizację, takie jak ochrona przed zagrożeniami mobilnymi, analiza zagrożeń mobilnych, usługi weryfikacji aplikacji i zasady bezpieczeństwa mobilnego. W przypadku takich niezarządzanych urządzeń organizacja ma ograniczony wgląd w ich stan – również w sytuacji, gdy ich bezpieczeństwo zostanie naruszone przez złośliwy podmiot. Dlatego użytkownicy, którzy

naruszają zasady bezpieczeństwa w celu uzyskania nieautoryzowanego dostępu do zasobów przedsiębiorstwa z takich urządzeń, ryzykują udostępnienie złośliwym podmiotom wrażliwych danych, usług i systemów organizacji.

F.1.7.11 Zdarzenie powodujące zagrożenie 11 — Utrata danych organizacji z powodu zgubienia lub kradzieży urządzenia

Ze względu na niewielkie rozmiary, urządzenia mobilne mogą zostać zgubione lub skradzione. Złośliwy podmiot, który uzyska fizyczną kontrolę nad urządzeniem z nieodpowiednimi zabezpieczeniami, może uzyskać nieautoryzowany dostęp do wrażliwych danych lub zasobów dostępnych dla tego urządzenia.

F.1.7.12 Zdarzenie powodujące zagrożenie 11 — Utrata poufności danych organizacji z powodu ich nieautoryzowanego przechowywania w usługach niezarządzanych przez organizację

Jeśli pracownik naruszy zasady zarządzania danymi, korzystając z niezarządzanych usług do przechowywania wrażliwych danych organizacji, dane te znajdą się poza jej kontrolą i nie będzie ona już w stanie chronić ich poufności, integralności ani dostępności. Złośliwe podmioty, które naruszą bezpieczeństwo nieautoryzowanego konta usługi lub dowolnego systemu obsługującego to konto, mogą uzyskać nieautoryzowany dostęp do danych.

Co więcej, przechowywanie wrażliwych danych w niezarządzanej usłudze może narazić użytkownika lub organizację na postępowanie sądowe za naruszenie obowiązujących przepisów (np. o eksporcie kryptografii) i może skomplikować działania organizacji mające na celu uzyskanie środków zaradczych lub naprawienie wszelkich przyszłych strat, takich jak te wynikające z publicznego ujawnienia tajemnic handlowych.

F.1.8 Zadanie 2-3: Identyfikacja podatności i warunków predysponujących

Identyfikacja podatności i warunków predysponujących, które wpływają na prawdopodobieństwo, że zdarzenia powodujące zagrożenia doprowadzą do negatywnych skutków.

Zgodnie ze scenariuszem opisanym w punkcie 3.4.3, istnieją podatności i warunki predysponujące, które zwiększają prawdopodobieństwo, że zidentyfikowane

zdarzenia powodujące zagrożenia będą miały negatywny wpływ na firmę Orvilia. Wszystkie podatności lub warunki predysponujące są wymienione w poniższej tabeli wraz z odpowiadającymi im zdarzeniami powodującymi zagrożenie.

Metodologia zastosowana do oceny poziomu powszechności była jakościowa (tj. subiektywna) i wykorzystano w niej pięciopunktową skalę.

- Bardzo wysoka
- Wysoka
- Umiarkowana
- Niska
- Bardzo niska

Tabela F-3 Identyfikacja podatności i warunków predysponujących

Identyfikator podatności	Podatność lub warunek predysponujący	Wynikowe zdarzenia powodujące zagrożenie	Powszechność
VULN-1	Dostęp do poczty elektronicznej i innych zasobów przedsiębiorstwa jest możliwy z dowolnego miejsca, a wymagane jest jedynie uwierzytelnienie za pomocą nazwy użytkownika/hasła.	TE-2, TE-10, TE-11	Bardzo wysoka
VULN-2	Pracownicy regularnie korzystają z publicznych sieci Wi-Fi w celu nawiązania zdalnej łączności z firmowych urządzeń mobilnych.	TE-7	Bardzo wysoka
VULN-3	Nie wdrożono systemu EMM/MDM, aby egzekwować i monitorować zgodność z zasadami bezpieczeństwa dotyczącymi firmowych urządzeń mobilnych.	TE-1, TE-3, TE-4, TE-5, TE-6, TE-7, TE-8, TE-9, TE-11, TE-12	Bardzo wysoka

Uwaga 1: Oceny poziomu powszechności oparto na skali jakościowej znajdującej się w tabeli F-5 załącznika F do publikacji NIST SP 800-30 w wersji 1 [12].

Uwaga 2: Oceny powszechności wskazują, że podatności dotyczą bardzo małej liczby (tj. bardzo niska), niewielu (tj. niska), wielu (tj. umiarkowana), dużej liczby (tj. wysoka)

lub wszystkich (tj. bardzo wysoka) misji/funkcji i procesów biznesowych organizacji lub systemów IT.

F.1.9 Zadanie 2-4: Określenie prawdopodobieństwa wystąpienia zagrożenia i prawdopodobieństwa jego negatywnych skutków

Określenie prawdopodobieństwa, że zdarzenia powodujące zagrożenia spowodują negatywne skutki, z uwzględnieniem (I) charakterystyki źródeł zagrożeń, które mogą je zainicjować; (II) zidentyfikowanych podatności/warunków predysponujących oraz (III) podatności organizacji z uwzględnieniem zabezpieczeń/środków zaradczych zaplanowanych lub wdrożonych w celu przeciwdziałania takim zdarzeniom.

Dla zachowania zwięzłości, główne zdarzenia powodujące zagrożenia zidentyfikowane w zadaniu 2-2 zostały ograniczone do tych, co do których przypuszcza się, że mają wysokie prawdopodobieństwo wystąpienia.

Metodologia zastosowana do określenia prawdopodobieństwa wystąpienia głównych zagrożeń była jakościowa (tj. subiektywna) i wykorzystano następującą pięciopunktową skalę.

- Bardzo wysokie
- Wysokie
- Umiarkowane
- Niskie
- Bardzo niskie

Tabela F-4 Prawdopodobieństwo wystąpienia głównych zdarzeń powodujących zagrożenia

Identyfikator zagrożenia	Prawdopodobieństwo zainicjowania zdarzenia powodującego zagrożenie	Prawdopodobieństwo wystąpienia negatywnych skutków zdarzenia powodującego zagrożenie	Ogólne prawdopodobieństwo
TE-1	Wysokie	Bardzo wysokie	Bardzo wysokie
TE-2	Bardzo wysokie	Wysokie	Bardzo wysokie

Identyfikator zagrożenia	Prawdopodobieństwo zainicjowania zdarzenia powodującego zagrożenie	Prawdopodobieństwo wystąpienia negatywnych skutków zdarzenia powodującego zagrożenie	Ogólne prawdopodobieństwo
TE-3	Wysokie	Wysokie	Wysokie
TE-4	Umiarkowane	Bardzo wysokie	Wysokie
TE-5	Wysokie	Bardzo wysokie	Bardzo wysokie
TE-6	Umiarkowane	Wysokie	Umiarkowane
TE-7	Wysokie	Wysokie	Wysokie
TE-8	Umiarkowane	Wysokie	Wysokie
TE-9	Umiarkowane	Wysokie	Bardzo wysokie
TE-10	Wysokie	Bardzo wysokie	Bardzo wysokie
TE-11	Bardzo wysokie	Bardzo wysokie	Bardzo wysokie
TE-12	Wysokie	Wysokie	Wysokie

Uwaga 1: W przypadku prawdopodobieństwa zainicjowania zdarzenia powodującego zagrożenie, oceny interpretuje się w następujący sposób: umiarkowane = istnieje pewne prawdopodobieństwo, że złośliwy podmiot zainicjuje zdarzenie; wysokie = istnieje duże prawdopodobieństwo, że złośliwy podmiot zainicjuje zdarzenie; bardzo wysokie = jest niemal pewne, że złośliwy podmiot zainicjuje zdarzenie.

Uwaga 2: W przypadku prawdopodobieństwa wystąpienia negatywnych skutków zdarzenia powodującego zagrożenie, oceny interpretuje się w następujący sposób: umiarkowane = jeśli zagrożenie zostanie zainicjowane, istnieje pewne prawdopodobieństwo, że będzie miało negatywne skutki; wysokie = jeśli zagrożenie zostanie zainicjowane, istnieje duże prawdopodobieństwo, że będzie miało negatywne skutki; bardzo wysokie = jeśli zagrożenie zostanie zainicjowane, jest niemal pewne, że będzie miało negatywne skutki.

Uwaga 3: Ogólne prawdopodobieństwo zostało obliczone na podstawie skali jakościowej zawartej w tabeli G-3 załącznika G do publikacji NIST SP 800-30 w wersji 1 [12]. Jest on pochodną zarówno prawdopodobieństwa zainicjowania zdarzenia powodującego zagrożenie, jak i prawdopodobieństwa wystąpienia negatywnych

skutków zdarzenia powodującego zagrożenie. Ponieważ skale te nie są prawdziwymi skalami interwałowymi, łączne oceny ogólne nie zawsze ściśle odpowiadają matematycznej średniej dwóch ocen.

F.1.10 Zadanie 2-5: Określenie stopnia negatywnych skutków

Określenie negatywnych skutków zdarzeń powodujących zagrożenie, biorąc pod uwagę (I) charakterystykę źródeł zagrożeń, które mogą zainicjować zdarzenia; (II) zidentyfikowane podatności/warunki predysponujące; oraz (III) podatność uwzględniającą zabezpieczenia/ środki zaradcze zaplanowane lub wdrożone w celu przeciwdziałania takim zdarzeniom.

Następnie w naszym scenariuszu zidentyfikowano zdarzenia powodujące zagrożenia o wysokim potencjale wywołania negatywnych skutków.

Metodologia zastosowana do określenia stopnia negatywnych skutków była jakościowa (tj. subiektywna) i wykorzystano następującą pięciopunktową skalę.

- Bardzo wysokie
- Wysokie
- Umiarkowane
- Niskie
- Bardzo niskie

Tabela F-5 Potencjalne negatywne skutki

Identyfikator zagrożenia	Rodzaj skutków	Aktywa, których dotyczy skutek	Maksymalny wpływ
TE-1	Szkody dla działalności, aktywów, osób fizycznych	Niezdolność lub ograniczona zdolność do wykonywania misji/funkcji biznesowych w przyszłości Uszkodzenie lub utrata systemów IT lub sieci	Wysoki
TE-2	Szkody dla działalności, innych organizacji	Niezdolność lub ograniczona zdolność do wykonywania misji/funkcji biznesowych w przyszłości	Wysoki

Identyfikator zagrożenia	Rodzaj skutków	Aktywa, których dotyczy skutek	Maksymalny wpływ
TE-3	Szkody dla działalności, aktywów	Niezdolność lub ograniczona zdolność do wykonywania misji/funkcji biznesowych w przyszłości Uszkodzenie lub utrata systemów IT lub sieci	Wysoki
TE-4	Szkody dla działalności, aktywów	Niezdolność lub ograniczona zdolność do wykonywania misji/funkcji biznesowych w przyszłości Uszkodzenie lub utrata systemów IT lub sieci	Wysoki
TE-5	Szkody dla działalności, aktywów, osób fizycznych	Niezdolność lub ograniczona zdolność do wykonywania misji/funkcji biznesowych w przyszłości Uszkodzenie lub utrata systemów IT lub sieci Utrata danych osobowych	Wysoki
TE-6	Szkody dla działalności, aktywów, innych organizacji	Niezdolność lub ograniczona zdolność do wykonywania misji/funkcji biznesowych w przyszłości Uszkodzenie lub utrata systemów IT lub sieci Nadszarpnięcie reputacji (a tym samym ograniczenie zdolności do nawiązywania przyszłych lub potencjalnych relacji opartych na zaufaniu)	Bardzo wysoki
TE-7	Szkody dla działalności, aktywów	Niezdolność lub ograniczona zdolność do wykonywania misji/funkcji biznesowych w przyszłości Uszkodzenie lub utrata systemów IT lub sieci	Wysoki
TE-8	Szkody dla działalności, aktywów	Niezdolność lub ograniczona zdolność do wykonywania misji/funkcji biznesowych w przyszłości Uszkodzenie lub utrata systemów IT lub sieci	Wysoki

Identyfikator zagrożenia	Rodzaj skutków	Aktywa, których dotyczy skutek	Maksymalny wpływ
TE-9	Szkody dla działalności, aktywów	Niezdolność lub ograniczona zdolność do wykonywania misji/funkcji biznesowych w przyszłości Uszkodzenie lub utrata systemów IT lub sieci	Wysoki
TE-10	Szkody dla działalności, aktywów	Niezdolność lub ograniczona zdolność do wykonywania misji/funkcji biznesowych w przyszłości Uszkodzenie lub utrata systemów IT lub sieci	Wysoki
TE-11	Szkody dla działalności, aktywów, osób fizycznych	Niezdolność lub ograniczona zdolność do wykonywania misji/funkcji biznesowych w przyszłości Uszkodzenie lub utrata systemów IT lub sieci Nadszarpnięcie reputacji (a tym samym ograniczenie zdolności do nawiązywania przyszłych lub potencjalnych relacji opartych na zaufaniu) Utrata danych osobowych	Wysoki
TE-12	Szkody dla działalności, aktywów, innych organizacji, osób fizycznych	Niezdolność lub ograniczona zdolność do wykonywania misji/funkcji biznesowych w przyszłości Uszkodzenie lub utrata systemów IT lub sieci Utrata danych osobowych Nadszarpnięcie reputacji (a tym samym ograniczenie zdolności do nawiązywania przyszłych lub potencjalnych relacji opartych na zaufaniu)	Wysoki

Uwaga 1: Oceny maksymalnego wpływu oparto na skali jakościowej znajdującej się w tabeli H-3 załącznika H do publikacji NIST SP 800-30 w wersji 1 [12].

Uwaga 2: Oceny maksymalnego wpływu wskazują, że zdarzenie powodujące zagrożenie może mieć nieistotne (tj. bardzo niskie ryzyko), ograniczone (niskie), poważne (umiarkowane), dotkliwe lub katastrofalne (wysokie), do wielu dotkliwych lub katastrofalnych skutków (bardzo wysokie).

Uwaga 3: Konkretne przykłady rodzajów wpływu można znaleźć w załączniku H do publikacji NIST SP 800-30 w wersji 1 [12].

F.1.11 Zadanie 2-6: Określenie ryzyka dla organizacji

Określenie ryzyka dla organizacji wynikającego ze zdarzeń powodujących zagrożenia, biorąc pod uwagę (I) skutki, które mogłyby wyniknąć z tych zdarzeń; oraz (II) prawdopodobieństwo wystąpienia tych zdarzeń.

Dla zachowania zwięzłości, główne zdarzenia powodujące zagrożenia zidentyfikowane w zadaniu 2-2 zostały ograniczone do tych, co do których przypuszcza się, że mają wysokie prawdopodobieństwo wystąpienia i doprowadzenia do negatywnych skutków w scenariuszu z firmą Orvilia.

Charakterystyka źródeł zagrożeń

W poniższej tabeli podsumowano ustalenia wynikające z szacowania ryzyka.

Metodologia zastosowana do określenia ryzyka dla organizacji była jakościowa (tj. subiektywna) i wykorzystano następującą pięciopunktową skalę.

- Bardzo wysokie
- Wysokie
- Umiarkowany
- Niskie
- Bardzo niskie

Tabela F-6 Podsumowanie wyników szacowania ryzyka

Zdarzenie powodujące zagrożenie	Podatności, warunki predysponujące	Ogólne prawdopodobieństwo	Poziom wpływu	Ryzyko
TE-1: Nieautoryzowany dostęp do wrażliwych informacji za pośrednictwem złośliwej lub naruszającej prywatność aplikacji	VULN-3	Bardzo wysokie	Wysokie	Wysokie

Zdarzenie powodujące zagrożenie	Podatności, warunki predysponujące	Ogólne prawdopodobieństwo	Poziom wpływu	Ryzyko
TE-2: Kradzież danych uwierzytelniających poprzez kampanię wyłudzania informacji za pośrednictwem wiadomości SMS lub e-mail.	VULN-1	Bardzo wysokie	Wysokie	Wysokie
TE-3: Złośliwe aplikacje zainstalowane za pośrednictwem adresów URL w wiadomościach SMS lub e-mail.	VULN-3	Wysokie	Wysokie	Wysokie
TE-4: Utrata poufności i integralności w wyniku wykorzystania znanej podatności w systemie operacyjnym lub oprogramowaniu układowym.	VULN-3	Wysokie	Wysokie	Wysokie
TE-5: Naruszenie prywatności poprzez niewłaściwe wykorzystanie czujników urządzenia.	VULN-3	Bardzo wysokie	Wysokie	Wysokie
TE-6: Naruszenie integralności urządzenia lub jego komunikacji sieciowej poprzez instalację złośliwego systemu EMM/MDM, sieci, profili VPN lub certyfikatów.	VULN-3	Umiarkowane	Bardzo wysokie	Wysokie
TE-7: Utrata poufności wrażliwych informacji poprzez podsłuchiwanie niezaszyfrowanej komunikacji urządzenia.	VULN-2	Wysokie	Wysokie	Wysokie
TE-8: Naruszenie integralności urządzenia poprzez zastosowanie kodu odblokowującego, który został zaobserwowany, wywnioskowany lub pozyskany na drodze ataku siłowego.	VULN-3	Wysokie	Wysokie	Wysokie

Zdarzenie powodujące zagrożenie	Podatności, warunki predysponujące	Ogólne prawdopodobieństwo	Poziom wpływu	Ryzyko
TE-9: Nieautoryzowany dostęp do usług zaplecza poprzez luki w uwierzytelnianiu lub przechowywaniu danych uwierzytelniających w wewnętrznie opracowanych aplikacjach.	VULN-3	Bardzo wysokie	Wysokie	Wysokie
TE-10: Nieautoryzowany dostęp do zasobów przedsiębiorstwa z urządzenia niezarządzanego i narażonego na naruszenie bezpieczeństwa.	VULN-1	Bardzo wysokie	Wysokie	Wysokie
TE-11: Utrata danych organizacji z powodu zgubienia lub kradzieży urządzenia.	VULN-3	Bardzo wysokie	Wysokie	Wysokie
TE-12: Utrata poufności danych organizacji z powodu ich nieautoryzowanego przechowywania w usługach niezarządzanych przez organizację.	VULN-3	Wysokie	Wysokie	Wysokie

Uwaga 1: Ryzyko jest określane jakościowo w oparciu o skalę w tabeli I-2 załącznika i w publikacji NIST SP 800-30 w wersji 1[12].

Uwaga 2: Sama ocena ryzyka jest określana na podstawie zarówno ogólnego prawdopodobieństwa, jak i poziomu skutków przy użyciu tabeli I2 w załączniku I do publikacji NIST SP 800-30 w wersji 1 [12]. Ponieważ skale te nie są prawdziwymi skalami interwałowymi, łączne oceny ogólnego ryzyka z tabeli I-2 nie zawsze ściśle odpowiadają matematycznej średniej tych dwóch zmiennych. Widać to w powyższej tabeli, w której poziomy umiarkowane są ważniejsze niż inne oceny.

Uwaga 3: Oceny ryzyka odnoszą się do prawdopodobieństwa i poziomu niekorzystnego wpływu na działalność organizacji, jej aktywa, osoby fizyczne, inne organizacje lub państwo. Zgodnie z publikacją NIST SP 800-30 w wersji 1, negatywne skutki (i związane z nimi ryzyko) wahają się od nieistotnych (tj. bardzo niskie ryzyko), ograniczonych (niskie), poważnych (umiarkowane), dotkliwych lub katastrofalnych (wysokie), do wielu dotkliwych lub katastrofalnych skutków (bardzo wysokie).

ZAŁĄCZNIK G SZACOWANIE RYZYKA DLA PRYWATNOŚCI

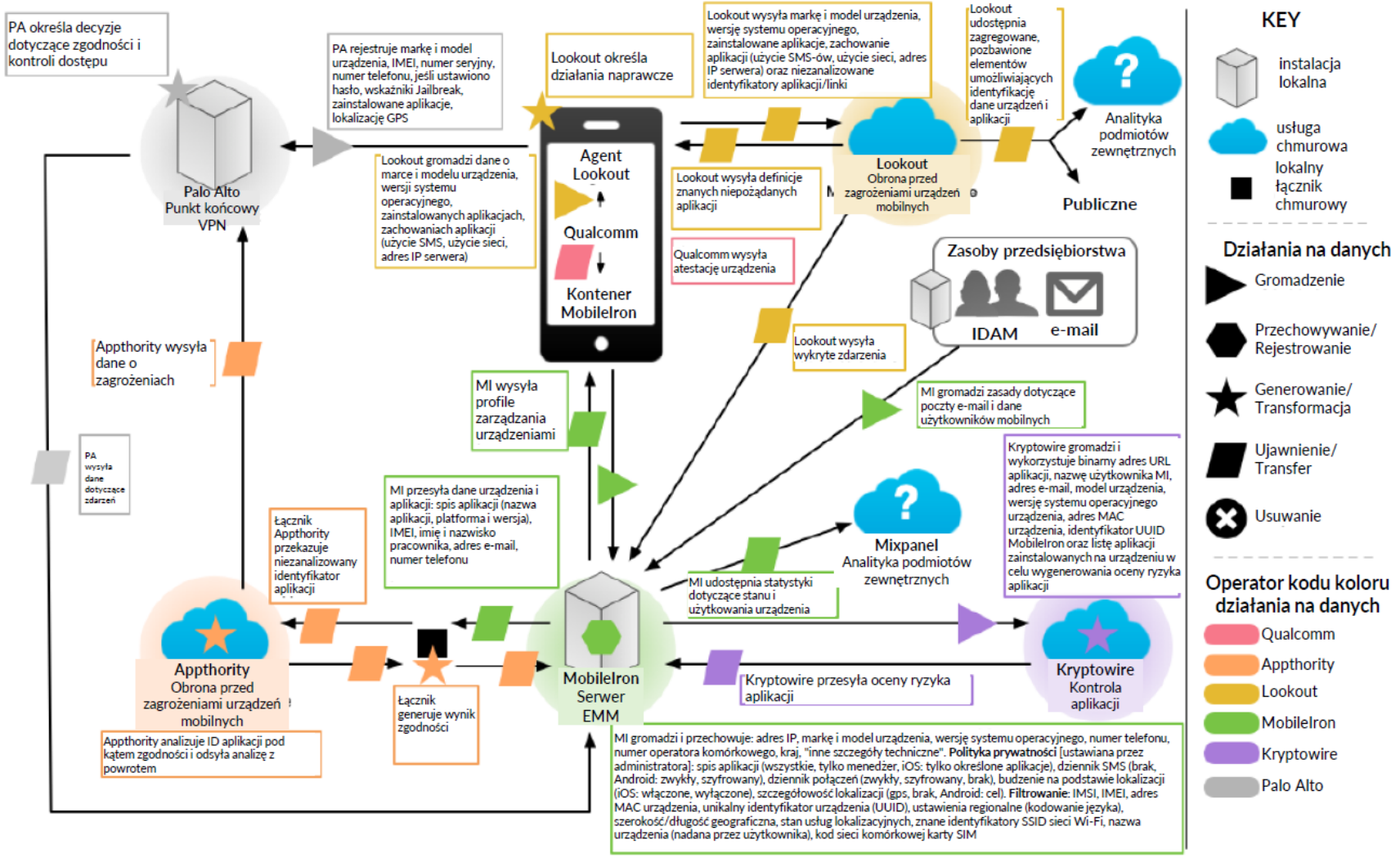
W tym punkcie opisano szacowanie ryzyka dla prywatności przeprowadzane w odniesieniu do architektury bezpieczeństwa przedsiębiorstwa Orvilia. W celu przeprowadzenia szacowania ryzyka dla prywatności wykorzystano metodologię szacowania ryzyka dla prywatności (*ang. Privacy Risk Assessment Methodology – PRAM*) Narodowego Instytutu Standardów i Technologii (NIST), narzędzie do analizy, oceny i priorytetyzacji zagrożeń dla prywatności, które ułatwia organizacjom określenie sposobu reagowania na nie i wybór odpowiednich rozwiązań. PRAM może również służyć jako użyteczne narzędzie komunikacyjne do informowania o zagrożeniach dla prywatności w organizacji. Pusta wersja PRAM jest dostępna do pobrania na stronie internetowej NIST [19].

Do analizy problematycznych działań związanych z danymi w ramach PRAM wykorzystywany jest model ryzyka dla prywatności i cele inżynierii prywatności opisane w raporcie wewnętrznym NIST IR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [20]. Działania na danych to wszelkie operacje systemowe, w ramach których przetwarzane są dane osobowe. Przetwarzanie może obejmować gromadzenie, przechowywanie, rejestrowanie, analizowanie, generowanie, przekształcanie lub łączenie, ujawnianie, przekazywanie i usuwanie danych osobowych. Problematyczne działanie na danych to takie, które może mieć niekorzystny wpływ na konkretne osoby.

Proces PRAM rozpoczyna się od określenia celów biznesowych systemu, w tym zaspokajanych przez niego potrzeb organizacji, oraz ustalenia zasad zarządzania prywatnością w organizacji, w tym identyfikacji obowiązków prawnych związanych z prywatnością oraz zobowiązań do przestrzegania zasad lub innych polityk organizacyjnych. Następnie tworzy się mapę danych w celu zilustrowania działań na danych wykonywanych przez system oraz danych osobowych przetwarzanych w ramach tych działań. Te działania na danych, przetwarzane dane osobowe oraz czynniki kontekstowe, które opisują okoliczności związane z przetwarzaniem danych osobowych przez system, służą jako dane wejściowe do analizy ryzyka.

Następnie należy oszacować prawdopodobieństwo, że działanie na danych stanie się problematyczne dla osób fizycznych, oszacować koszty wtórne ponoszone przez organizację w związku z takim działaniem stwarzającym problem dla osób fizycznych oraz wykorzystać obliczenia prawdopodobieństwa i wpływu w celu określenia całkowitego szacowanego ryzyka dla każdego działania związanego z danymi. Na koniec należy sporządzić listę potencjalnych technicznych środków i zasad mogących przeciwdziałać zidentyfikowanym zagrożeniom. Wynikiem działań w ramach procesu PRAM są informacje zawarte na rysunku G-1.

Uwaga: Legenda do rysunku G-1 obejmuje wszystkie typy działań na danych (gromadzenie, przechowywanie/rejestrowanie, generowanie/przekształcanie, ujawnianie/przekazywanie i usuwanie), ale to konkretne przykładowe rozwiązanie nie obejmuje usuwania danych w ćwiczeniu mapowania danych osobowych.



Rysunek G-1 Mapa danych PRAM dla architektury bezpieczeństwa przedsiębiorstwa Orvilia

Jako wynik procesu PRAM dla firmy Orvilia zidentyfikowaliśmy trzy ogólne działania na danych, które mogą stwarzać problemy dla osób fizycznych, oraz odpowiednie środki zaradcze. Niektóre środki zaradcze wymienione pod konkretnym działaniem na danych mogą zapewniać korzyści w zakresie prywatności osobom fizycznym wykraczające poza zakres tego działania. Zidentyfikowaliśmy również nadrzędne środki związane ze szkoleniami i wsparciem, które mogą ograniczyć ryzyko związane ze wszystkimi trzema działaniami na danych.

Chociaż funkcja bezpieczeństwa informacji i zarządzania zdarzeniami (*ang. Security Information and Event Management – SIEM*) nie została wykorzystana w implementacji referencyjnej, narzędzia SIEM, jak omówiono tutaj, mogą być niezwykle korzystne dla zrozumienia implikacji rejestrowania, agregowania i przechowywania danych dotyczących bezpieczeństwa urządzeń mobilnych dla prywatności.

G.1 DZIAŁANIE NA DANYCH 1: BLOKOWANIE DOSTĘPU I WYMAZYWANIE PAMIĘCI URZĄDZEŃ

W przypadku urządzeń, które mogą stanowić zagrożenie dla bezpieczeństwa organizacji, można zablokować dostęp do zasobów przedsiębiorstwa lub wymazać ich pamięć i przywrócić ustawienia fabryczne. W kolejnych punktach przedstawiono sposoby, w jakie można tego dokonać.

G.1.1 Potencjalne problemy dla osób fizycznych

W środowisku, w którym należące do firmy urządzenia są udostępniane pracownikom lub są ich własnością, pracownicy będą prawdopodobnie używać tych urządzeń zarówno do celów osobistych, jak i związanych z pracą. Dlatego, jeśli system ma możliwość całkowitego wymazania pamięci urządzenia, może dojść do utraty osobistych danych przez pracowników, a oni mogą nawet nie zdawać sobie sprawy z takiej możliwości. Hipotetycznym przykładem może być sytuacja, w której pracownik firmy Orvilia przechowuje osobiste zdjęcia na urządzeniu mobilnym wydanym mu przez to przedsiębiorstwo, ale zdjęcia te zostają utracone, gdy pamięć jego urządzenia zostaje wyczyszczona po wykryciu anomalnej aktywności.

G.1.2 Środki zaradcze[8]

Blokowanie dostępu zamiast wymazywania pamięci urządzeń.

Alternatywą dla całkowitego wymazywania danych może być zablokowanie urządzeniom dostępu do zasobów przedsiębiorstwa, na przykład do czasu usunięcia niezatwierdzonej aplikacji. Taka czasowa blokada dostępu umożliwia zapewnienie, że dana osoba nie utraci prywatnych danych w wyniku całkowitego wyczyszczenia pamięci urządzenia. Przyjęcie takiego podejścia może pomóc w dostosowaniu działania systemu do oczekiwań pracowników dotyczących tego, co może się stać z ich urządzeniami, zwłaszcza jeśli nie są świadomi, że pamięć urządzeń może zostać wyczyszczona przez administratorów – zapewnia to większą przewidywalność działania systemu.

- Powiązany środek zaradczy: Jeśli zostanie przyjęte takie podejście, należy również opracować procesy naprawcze i poinformować o nich pracowników. Ważne jest, aby wdrożyć jasny proces naprawczy, aby pomóc pracownikom odzyskać dostęp do zasobów z ich urządzeń w odpowiednim czasie. Równie ważne jest jasne przekazanie informacji na temat tego procesu pracownikom. Proces naprawczy ułatwia zarządzanie systemem, wspierając dostęp pracowników do zasobów. Jeśli informacje o nim zostaną we właściwy sposób przekazane pracownikom, zapewnia to również większą przewidywalność, ponieważ będą oni wiedzieć, jakie kroki należy podjąć w celu odzyskania dostępu.

Włączenie wyłącznie funkcji czyszczenia selektywnego.

Alternatywną opcją łagodzenia skutków czyszczenia pamięci urządzenia jest określenie informacji, które mają zostać usunięte. Selektywne czyszczenie (*ang. wiping*) jest opcją, która umożliwia usunięcie z urządzenia jedynie danych firmowych, a nie pełne przywrócenie ustawień fabrycznych. Po skonfigurowaniu w ten sposób, funkcja czyszczenia zachowuje osobiste konfiguracje, aplikacje i dane pracowników,

[8] Środek zaradczy – także: mitygacja (*ang. mitigation*).

jednocześnie usuwając tylko konfiguracje, aplikacje i dane firmowe. W przykładowym rozwiązaniu opcja ta jest dostępna dla urządzeń z systemem iOS;

Zalecanie pracownikom tworzenia kopii zapasowych osobistych danych przechowywanych na urządzeniach.

Jeśli czyszczenie pamięci urządzeń pozostaje dostępną opcją dla administratorów, należy zachęcać pracowników do regularnego tworzenia kopii zapasowych prywatnych danych, aby zapewnić ich dostępność w przypadku wymazania.

Ograniczenie pracownikom możliwości wymazywania danych lub blokowania dostępu.

Ograniczenie liczby pracowników z uprawnieniami do wymazywania danych tylko do tych, którzy są za to odpowiedzialni, poprzez zastosowanie kontroli dostępu opartej na rolach. Może to ograniczyć ryzyko przypadkowego usunięcia danych pracowników lub zablokowania dostępu do zasobów.

G.2 DZIAŁANIE NA DANYCH 2: MONITOROWANIE PRACOWNIKÓW

Oceniana infrastruktura umożliwia firmie Orvilia korzystanie z szeregu funkcji bezpieczeństwa, w tym z kompleksowego monitorowania, jak opisano w punkcie 4, „Architektura”. Znaczna ilość danych dotyczących pracowników, ich urządzeń i działań jest gromadzona i analizowana przez wiele stron.

G.2.1 Potencjalne problemy dla osób fizycznych

Pracownicy mogą nie być świadomi, że ich interakcje z systemem są monitorowane i mogą nie chcieć, aby takie monitorowanie miało miejsce. Gromadzenie i analiza informacji mogą umożliwić firmie Orvilia lub innym stronom tworzenie narracji na temat pracownika w oparciu o jego interakcje z systemem, co może prowadzić do braku równowagi relacji między firmą Orvilia a pracownikiem i utraty zaufania do pracodawcy, jeśli pracownik odkryje nieoczekiwany monitoring.

G.2.2 Środki zaradcze

Ograniczenie personelowi możliwości przeglądania danych o pracownikach i ich urządzeniach. Można to osiągnąć za pomocą kontroli dostępu opartej na rolach i poprzez opracowanie zasad organizacji w celu ograniczenia sposobu, w jaki dane pracowników mogą być wykorzystywane przez personel mający do nich dostęp. Dostęp może być ograniczony do dowolnego pulpitu nawigacyjnego w systemie zawierającego dane o pracownikach i ich urządzeniach. Najbardziej wrażliwy jest jednak pulpit zarządzania urządzeniami mobilnymi, który stanowi centrum danych o pracownikach, ich urządzeniach i zagrożeniach. Zminimalizowanie dostępu do wrażliwych informacji może zwiększyć możliwość anonimizacji pracowników korzystających z systemu.

Ograniczenie lub wyłączenie gromadzenia określonych elementów danych.

Przeprowadzenie szacowania ryzyka dla prywatności specyficznego dla systemu w celu określenia, gromadzenie których elementów może być ograniczone. Należy rozważyć opcje konfiguracji dla inwazyjnych funkcji urządzeń, takich jak usługi lokalizacyjne, gromadzenie wykazu aplikacji i funkcje wybudzania oparte na lokalizacji. Podczas zbierania danych o aplikacjach należy upewnić się, że informacje są gromadzone wyłącznie z aplikacji zainstalowanych z firmowego sklepu z aplikacjami. Chociaż te konfiguracje administracyjne mogą pomóc w zapewnieniu anonimowości w systemie, istnieją również pewne opcje dla pracowników, aby ograniczyć gromadzenie danych.

Organizacje mogą zezwolić swoim pracownikom na zarządzanie niektórymi aspektami i konfiguracjami ich urządzeń. Na przykład, pracownicy mogą mieć możliwość wyłączenia usług lokalizacyjnych w systemie operacyjnym swojego urządzenia, aby zapobiec gromadzeniu danych o lokalizacji. Każdy z tych sposobów przyczynia się do zmniejszenia ilości gromadzonych danych dotyczących pracowników i ich urządzeń mobilnych. Ta redukcja gromadzenia danych skutkuje ograniczeniem zdolności administratorów do kojarzenia informacji z konkretnymi osobami.

Usuwanie danych osobowych.

Usuwanie danych osobowych po upływie odpowiedniego okresu przechowywania może ograniczać ryzyko tworzenia przez różne podmioty profili osób fizycznych. Może ono również umożliwić dostosowanie przetwarzania danych w systemie do oczekiwań pracowników i zmniejszyć ryzyko związane z przechowywaniem dużej ilości danych osobowych. Usuwanie może być szczególnie ważne dla niektórych stron w systemie, które gromadzą większą ilość danych lub bardziej wrażliwe dane. Usuwanie może być realizowane za pomocą kombinacji zasad i środków technicznych. Strony w systemie mogą określić, co dzieje się z danymi, kiedy i jak często są usuwane.

G.3 DZIAŁANIE NA DANYCH 3: UDOSTĘPNIANIE DANYCH MIĘDZY STRONAMI

Infrastruktura obejmuje kilka stron, które służą różnym zadaniom wspierającym cele bezpieczeństwa organizacji Orvilia. W związku z tym następuje znaczny przepływ danych dotyczących osób fizycznych i ich urządzeń między różnymi stronami. Obejmuje to udostępnianie danych urządzenia i aplikacji publicznie oraz zewnętrznym usługom analitycznym, a także udostępnianie statusu urządzenia i informacji o jego użytkowaniu takim usługom.

G.3.1 Potencjalne problemy dla osób fizycznych

Przesyłanie danych o osobach i ich urządzeniach między różnymi stronami może być kłopotliwe dla pracowników, którzy mogą nie wiedzieć, kto ma dostęp do różnych informacji na ich temat. Jeśli administratorzy i współpracownicy będą wiedzieli, który pracownik wykonuje na swoim urządzeniu działania, które wywołują alerty bezpieczeństwa, może to narazić pracownika na zakłopotanie lub stres emocjonalny. Ujawnienie takich informacji i powiązanie ich z konkretnymi osobami może również prowadzić do stygmatyzacji, a nawet wpłynąć na kierownictwo firmy Orvilia przy podejmowaniu decyzji dotyczących danego pracownika. Co więcej, przesyłanie danych w postaci zwykłego tekstu może powodować podatność na ataki i nieoczekiwane ujawnienie informacji o pracownikach.

G.3.2 Środki zaradcze

Stosowanie technik deidentyfikacji.

Deidentyfikacja danych umożliwia zmniejszenie prawdopodobieństwa, że strona trzecia będzie agregować informacje odnoszące się do jednej konkretnej osoby. Chociaż deidentyfikacja może ograniczyć ryzyko dla prywatności, istnieje szczątkowe ryzyko reidentyfikacji. Techniki deidentyfikacji mogą być stosowane do zagregowanych danych przed udostępnieniem ich zewnętrznym firmom analitycznym i na forum publicznym.

Stosowanie szyfrowania.

Szyfrowanie zmniejsza ryzyko przesyłania niezabezpieczonych informacji między stronami. Organizacje powinny o tym pamiętać, wybierając sposób przesyłania i przechowywania danych przedsiębiorstwa. Mobilne systemy bezpieczeństwa udostępniają sobie nawzajem dane urządzeń mobilnych i aplikacji w celu optymalizacji wydajności i wykorzystania danych do wykonywania funkcji bezpieczeństwa. Dane te mogą obejmować spis aplikacji oraz imię i nazwisko pracownika, adres e-mail i numer telefonu. Niektóre systemy umożliwiają szyfrowanie na wiele sposobów, co umożliwia organizacji wybór poziomu szyfrowania niezbędnego dla rodzaju przechowywanych lub przesyłanych danych.

Ograniczenie lub wyłączenie dostępu do danych.

Przeprowadzenie szacowania ryzyka dla prywatności specyficznego dla systemu w celu określenia, w jaki sposób można ograniczyć dostęp do danych. Korzystanie z kontroli dostępu w celu ograniczenia dostępu pracowników do informacji o przestrzeganiu zasad, zwłaszcza gdy dotyczą one konkretnych osób, jest ważne, aby zapobiec kojarzeniu określonych zdarzeń z poszczególnymi pracownikami, co mogłoby spowodować ich zakłopotanie. Produkty wykorzystywane przez organizację mogą obejmować opcje ograniczania ilości informacji o pracownikach, do których administrator ma dostęp. Opcje te mogą obejmować możliwość ukrycia nazwy użytkownika i adresu e-mail pracownika w konsoli administratora. Dane o aplikacjach

mobilnych również mogą obejmować informacje o pracownikach. Organizacje powinny rozważyć, czy ich systemy bezpieczeństwa urządzeń mobilnych i inne systemy bezpieczeństwa powinny ukrywać przed administratorami nazwy aplikacji, szczegółowe wyniki analizy binarnej aplikacji, identyfikatory zestawów usług nazw sieciowych i szczegółowe wyniki analizy sieci.

Ograniczenie lub wyłączenie gromadzenia określonych elementów danych.

Przeprowadzenie szacowania ryzyka dla prywatności specyficznego dla systemu w celu określenia, gromadzenie których elementów może być ograniczone. Określenie rodzaju gromadzonych informacji o pracownikach i ustalenie, jakie elementy danych są przechowywane, ułatwia szacowanie ryzyka dla prywatności związanego z mobilnymi systemami bezpieczeństwa. Organizacje powinny zwrócić uwagę na zdolność systemu bezpieczeństwa urządzeń mobilnych do limitowania lub ograniczania gromadzenia i przechowywania informacji o pracownikach, takich jak: nazwa użytkownika, adres e-mail, lokalizacja w systemie GPS i dane aplikacji.

Korzystanie z umów w celu ograniczenia przetwarzania danych przez strony trzecie.

Ustanowienie umownych zasad w celu ograniczenia przetwarzania danych przez strony trzecie wyłącznie do działań, które ułatwiają świadczenie usług związanych z bezpieczeństwem, oraz nieprzetwarzanie danych w innych celach niż wyraźnie określone.

G.4 ŚRODKI ZARADCZE MAJĄCE ZASTOSOWANIE DO RÓŻNYCH DZIAŁAŃ NA DANYCH

Kilka środków zaradczych jest korzystnych dla pracowników w odniesieniu do wszystkich trzech działań na danych zidentyfikowanych w ramach szacowania ryzyka związanego z prywatnością. Te środki związane ze szkoleniami i wsparciem mogą ułatwić firmie Orvilia przekazywanie pracownikom odpowiednich informacji na temat systemu i przetwarzania danych.

Środki zaradcze:

Zapewnienie pracownikom szkoleń na temat systemu, zaangażowanych stron, przetwarzania danych i działań administracyjnych, które mogą zostać podjęte.

W ramach sesji szkoleniowych można również zwrócić uwagę na wszelkie stosowane techniki ochrony prywatności, takie jak wykorzystywane w przypadku ujawniania informacji stronom trzecim. Szkolenie powinno obejmować uzyskanie od pracowników potwierdzenia, że rozumieją oni działania, które mogą zostać podjęte na ich urządzeniach i ich konsekwencje – niezależnie od tego, czy wiążą się one z zablokowaniem dostępu, czy wymazaniem danych. Pracownicy mogą być również poinformowani o okresach przechowywania danych i o tym, kiedy ich dane zostaną usunięte. Może to być bardziej skuteczne niż udostępnianie polityki prywatności, której, jak wykazały badania, nikt raczej nie czyta.

Zapewnienie ciągłych powiadomień lub przypomnień o działaniu systemu.

Można do tego celu wykorzystać powiadomienia typu „*push*”, podobne do tych przedstawionych na zrzutach ekranu w załączniku H, „Zdarzenie powodujące zagrożenie 6”, aby ułatwić bezpośrednie powiązanie działań administracyjnych na urządzeniach z odpowiednimi zagrożeniami i pomóc pracownikom zrozumieć, dlaczego dane działanie jest podejmowane. Powiadomienia o zmianach zasad mogą zwiększyć przewidywalność systemu odpowiednio dostosowując oczekiwania pracowników do sposobu, w jaki system przetwarza dane i wynikające z tego działania.

Zapewnienie punktu kontaktowego wsparcia.

Zapewnienie pracownikom punktu kontaktowego w organizacji, który może odpowiadać na zapytania i wątpliwości dotyczące systemu, umożliwia im lepsze zrozumienie przetwarzania ich danych przez system, co zwiększa jego przewidywalność.

ZAŁĄCZNIK H INFORMACJE O TESTACH ZDARZEŃ POWODUJĄCYCH ZAGROŻENIA

Poniżej znajdują się szczegółowe informacje i zrzuty ekranu dotyczące niektórych zdarzeń powodujących zagrożenia i wyniki związanych z nimi testów.

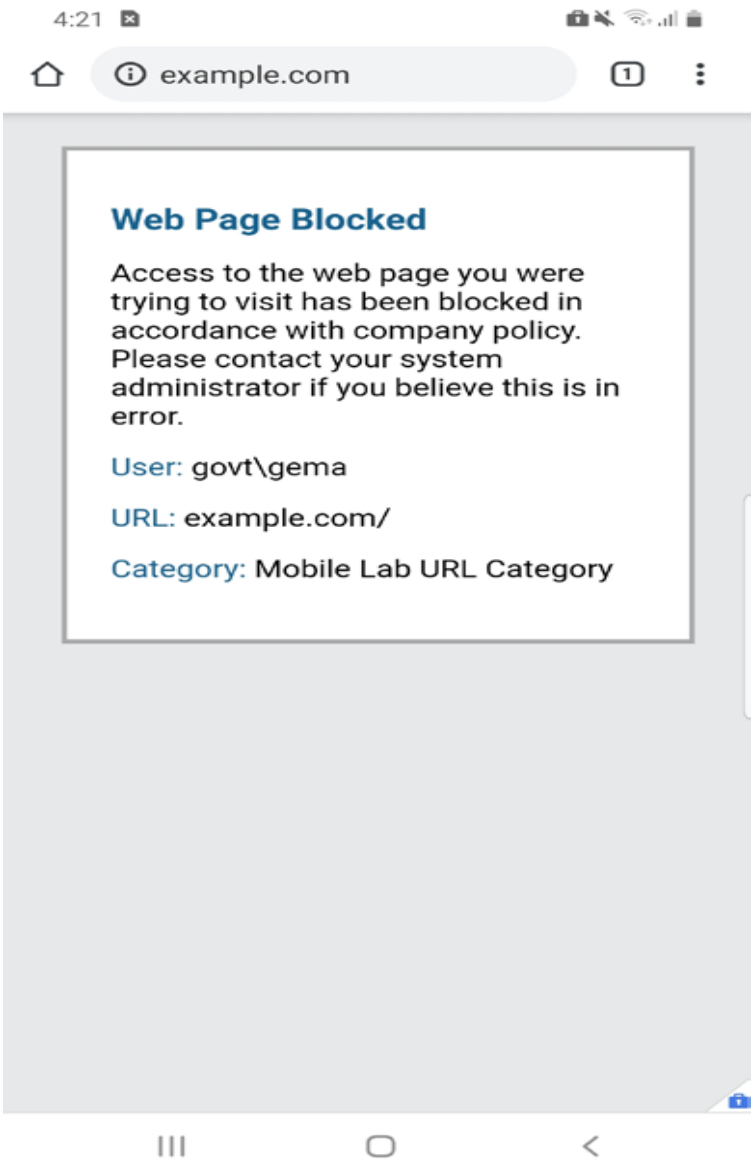
H.1 ZDARZENIE POWODUJĄCE ZAGROŻENIE 1 (TE-1) — NIEAUTORYZOWANY DOSTĘP DO POUFNYCH INFORMACJI ZA POŚREDNICTWEM ZŁOŚLIWEJ LUB NARUSZAJĄCEJ PRYWATNOŚĆ APLIKACJI

Część wniosków z testów zdarzenia powodującego zagrożenie nr 1 jest zaprezentowana na poniższym zrzucie ekranu, gdzie dla uprawnienia dostępu do kalendarza ustawiono ocenę ryzyka równą 10. Dzięki temu system MobileIron może automatycznie przypisać urządzeniu etykietę wysokiego ryzyka dla ochrony przed zagrożeniami mobilnymi i poddać je kwarantannie do czasu usunięcia aplikacji naruszającej prywatność.

Rysunek H-1 Ustawianie niestandardowego poziomu ryzyka w usłudze Appthority

H.2 ZDARZENIE POWODUJĄCE ZAGROŻENIE 2 — KRADZIEŻ DANYCH UWIERZYTELNIAJĄCYCH ZA POŚREDNICTWEM USŁUGI SMS LUB KAMPANII E-MAIL SŁUŻĄCEJ DO WYŁUDZANIA INFORMACJI

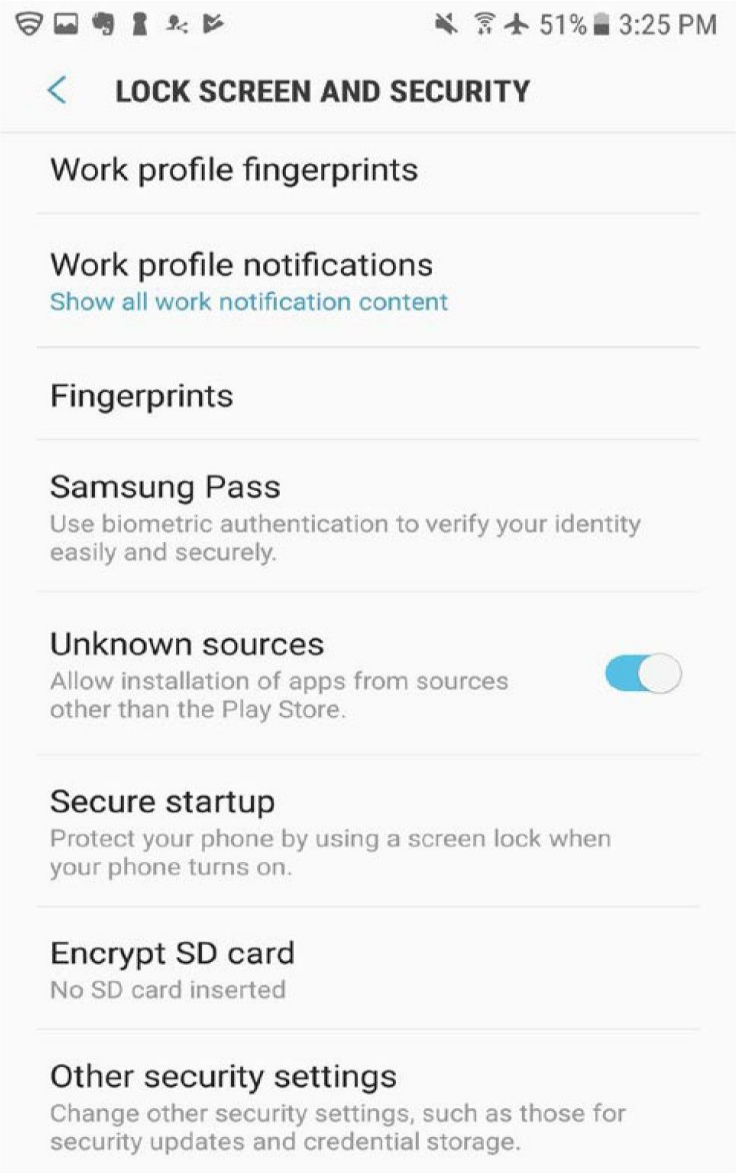
Na poniższym zrzucie ekranu przedstawiono wynik zdarzenia powodującego zagrożenie nr 2 – usługa PAN-DB blokuje witrynę ręcznie dodaną do bazy danych złośliwych adresów URL.



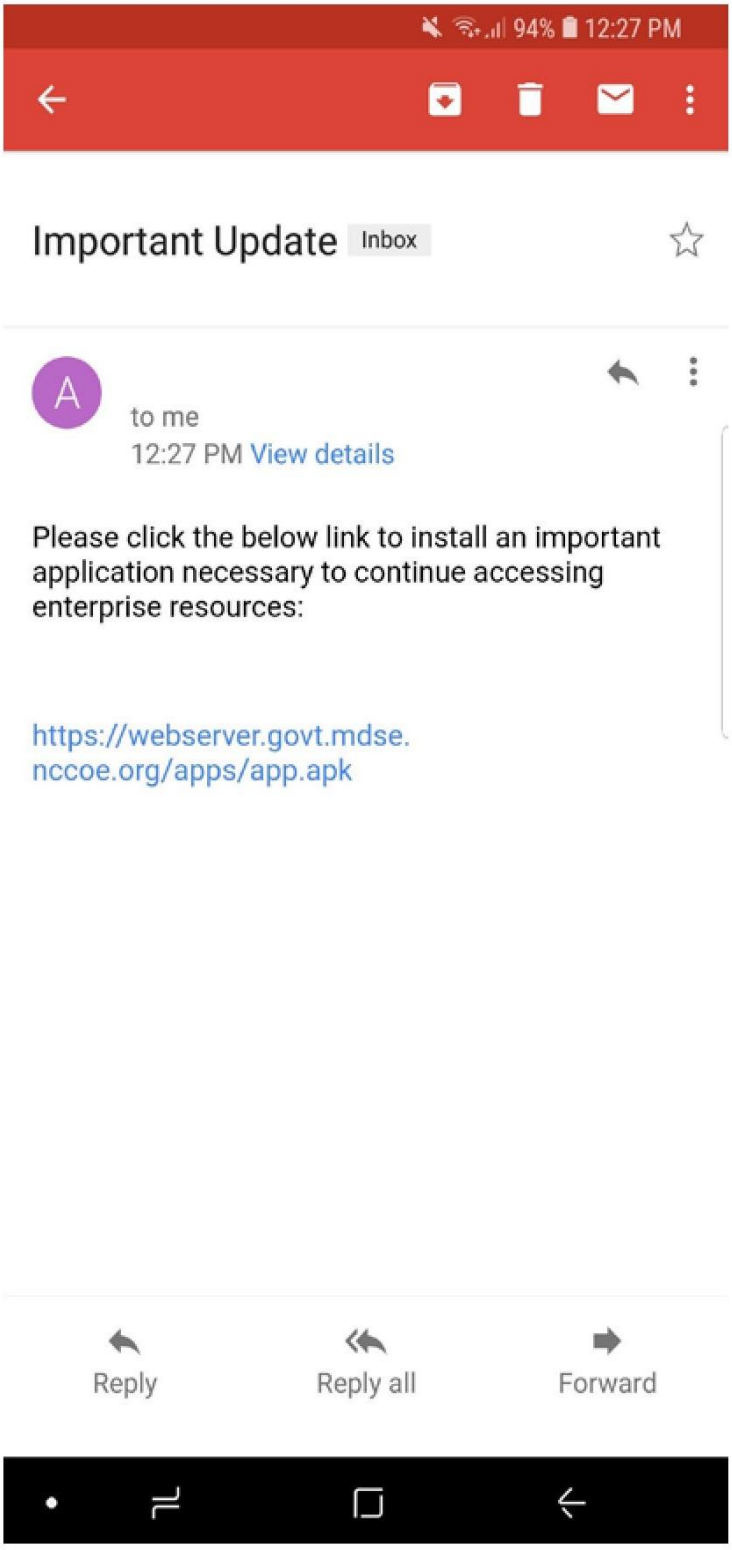
Rysunek H-2 Strona internetowa zablokowana przez usługę PAN-DB

H.3 ZDARZENIE POWODUJĄCE ZAGROŻENIE 3 — ZŁOŚLIWE APLIKACJE INSTALOWANE ZA POŚREDNICTWEM ADRESU URL W WIADOMOŚCIACH SMS LUB E-MAIL

Na poniższych zrzutach ekranu zademonstrowano włączanie przełącznika Unknown sources (Nieznane źródła) i instalowanie aplikacji za pośrednictwem łącza w wiadomości e-mail.

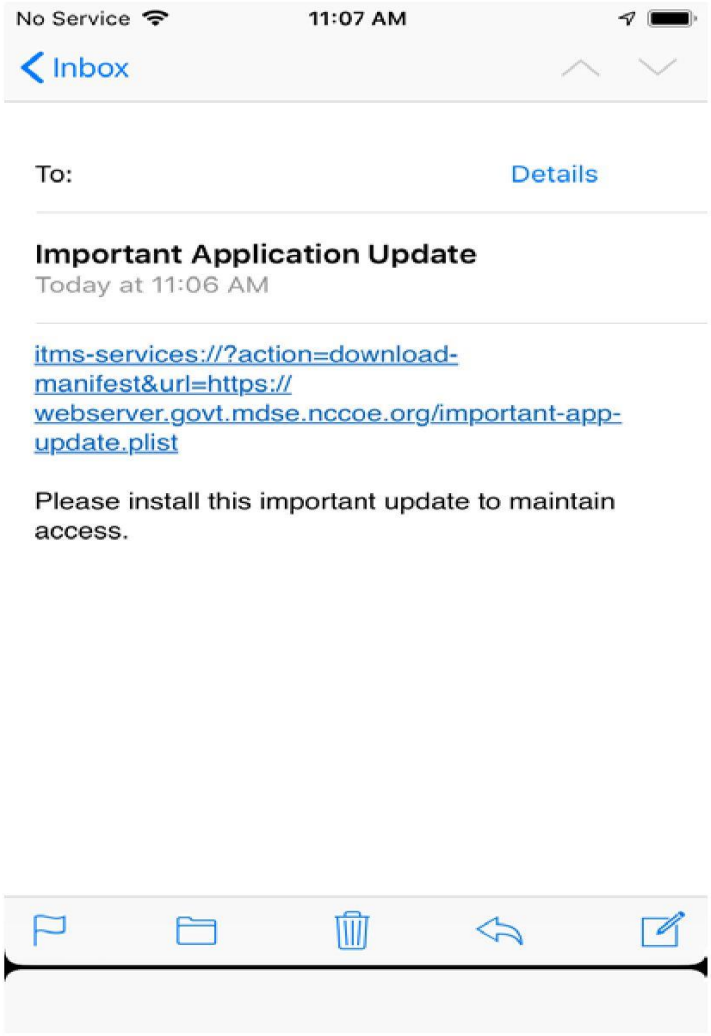


Rysunek H-3 Ekran blokady i zabezpieczenia



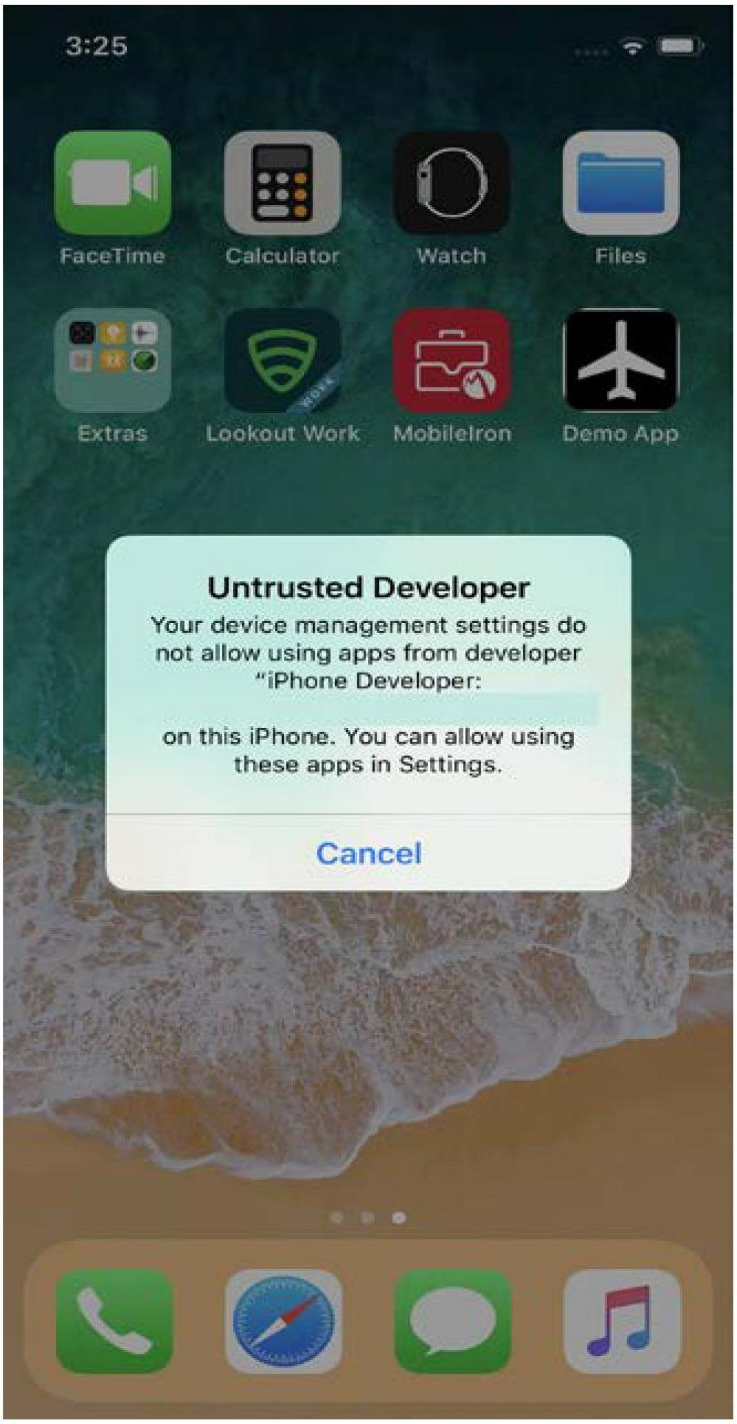
Rysunek H-4 Wiadomość z próbą wyłudzenia danych w systemie Android

Na rysunku H-5 przedstawiono testowe działanie w systemie iOS polegające na dostarczeniu wiadomości e-mail zawierającej łącze do aplikacji ze źródła spoza Apple App Store.



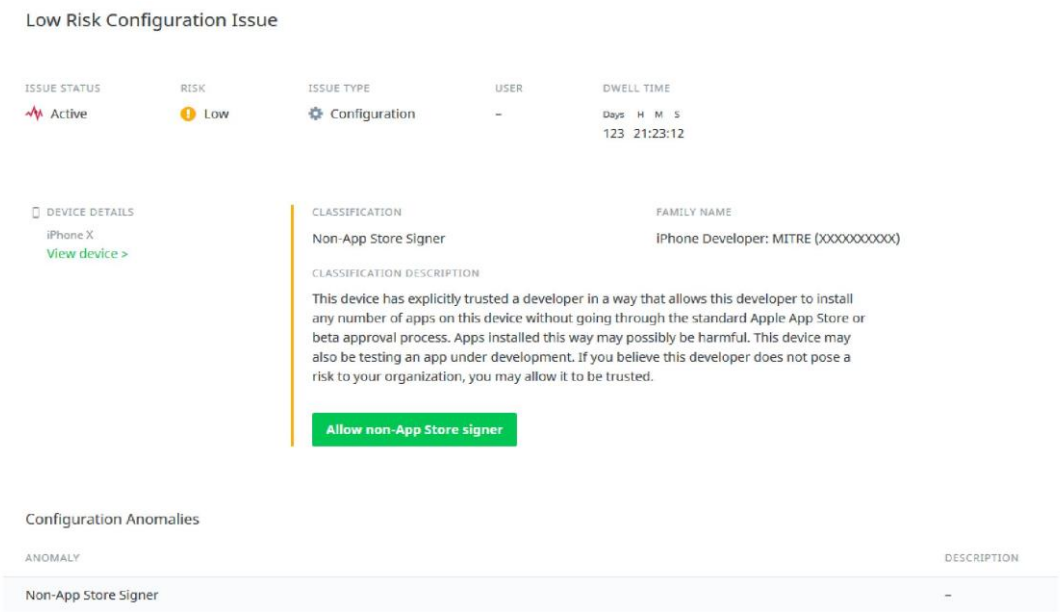
Rysunek H-5 Wiadomość z próbą wyłudzenia danych w systemie iOS

Po zainstalowaniu aplikacji, gdy użytkownik próbuje ją uruchomić, pojawia się komunikat o niezaufanym deweloperze, jak pokazano na rysunku H-6.



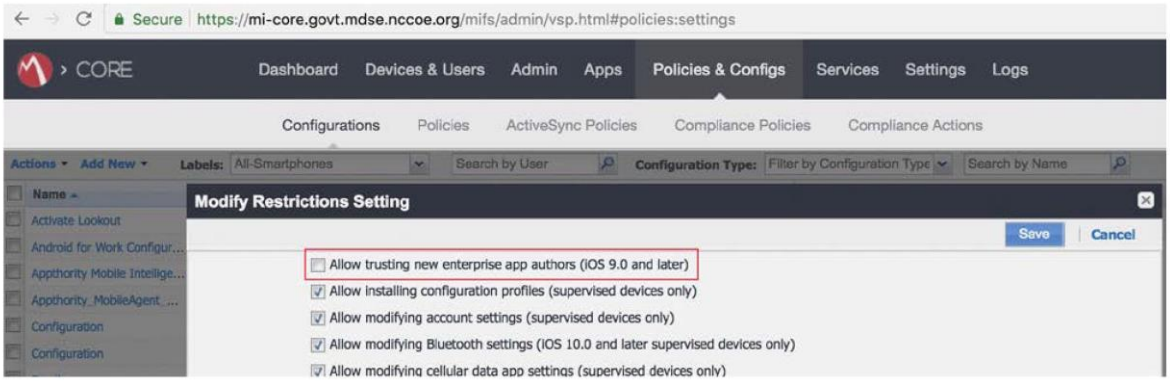
Rysunek H-6 Ostrzeżenie o niezaufanym deweloperze

Rysunek H-7 pokazuje zdolność Lookout do wykrywania certyfikatów podpisywania aplikacji, którym użytkownik zaufał na urządzeniu w celu uruchamiania aplikacji ze źródeł innych niż App Store firmy Apple.

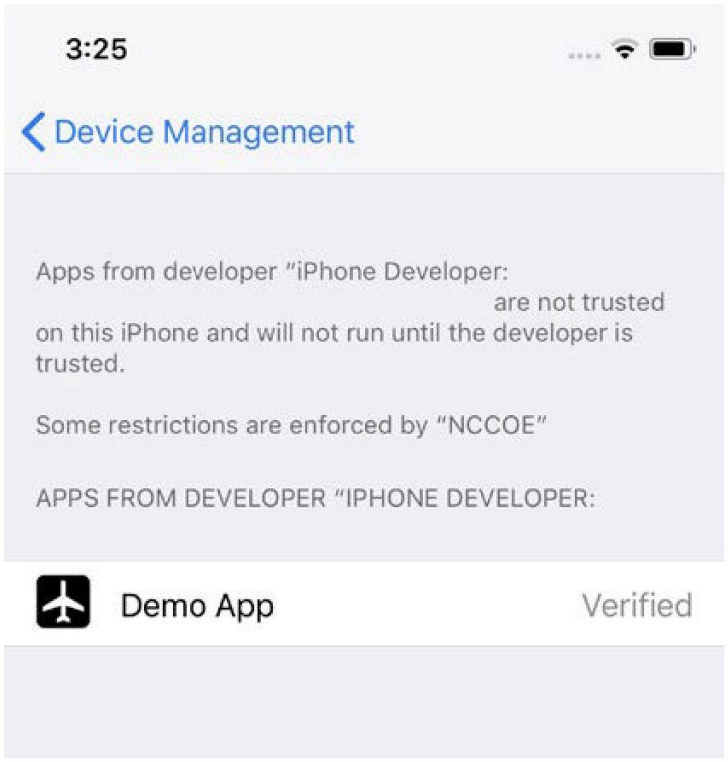


Rysunek H-7 Certyfikaty podpisywania aplikacji

Na poniższych zrzutach ekranu przedstawiono próbę zainstalowania i uruchomienia nieautoryzowanej aplikacji demonstracyjnej na urządzeniu z systemem iOS z ograniczeniem zasady `allowEnterpriseAppTrust` ustawionym na wartość „false” w systemie EMM. Użytkownik nie może zaufać deweloperowi, gdy ograniczenie zasady jest aktywne, a zatem aplikacja nie zostanie uruchomiona.



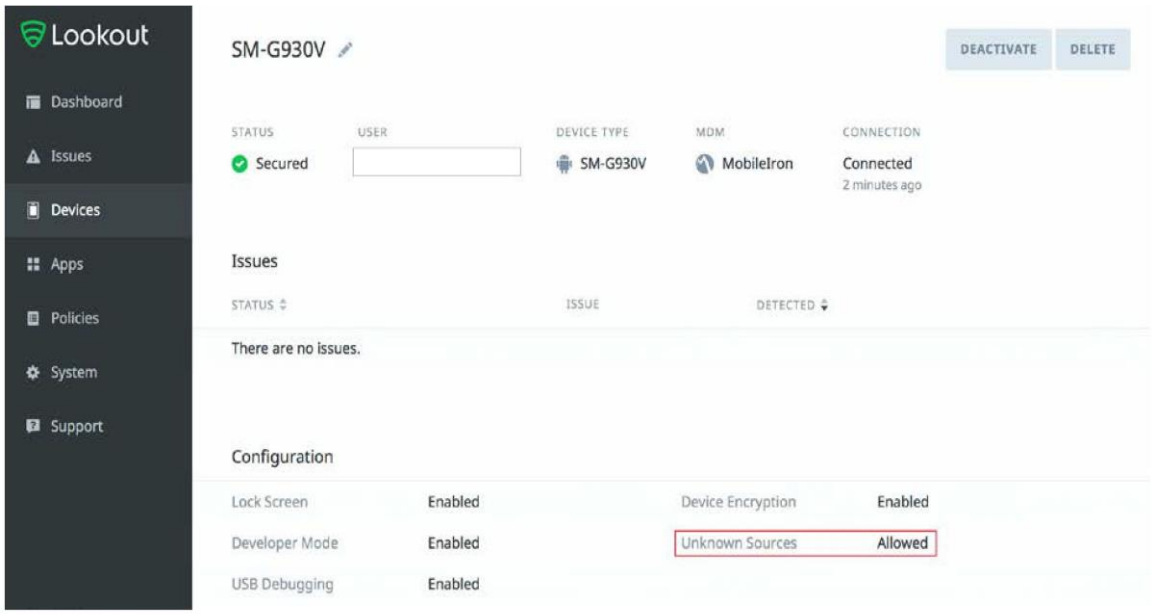
Rysunek H-8 Ekran modyfikacji ustawień ograniczeń



Rysunek H-9 Brak zaufania do dewelopera

Testowanie urządzeń z systemem Android

Na urządzeniach z systemem Android nie można instalować aplikacji ze źródeł innych niż sklep Google Play, chyba że w ustawieniach zabezpieczeń urządzenia włączono opcję Unknown sources (Nieznane źródła). Usługa Lookout może wykryć, że ustawienie to zostało włączone i może przekazać informację na ten temat do systemu MobileIron, aby umożliwić zautomatyzowane reakcje, takie jak zablokowanie dostępu urządzenia do zasobów przedsiębiorstwa do czasu rozwiązania problemu. Jednak nawet jeśli ustawienie Unknown sources (Nieznane źródła) jest wyłączone, możliwe jest, że było ono wcześniej włączone i w tym czasie zainstalowano nieautoryzowane aplikacje. Na rysunku H-10 przedstawiono funkcję wykrywania urządzeń z systemem Android z włączoną opcją Unknown sources (Nieznane źródła) usługi Lookout.

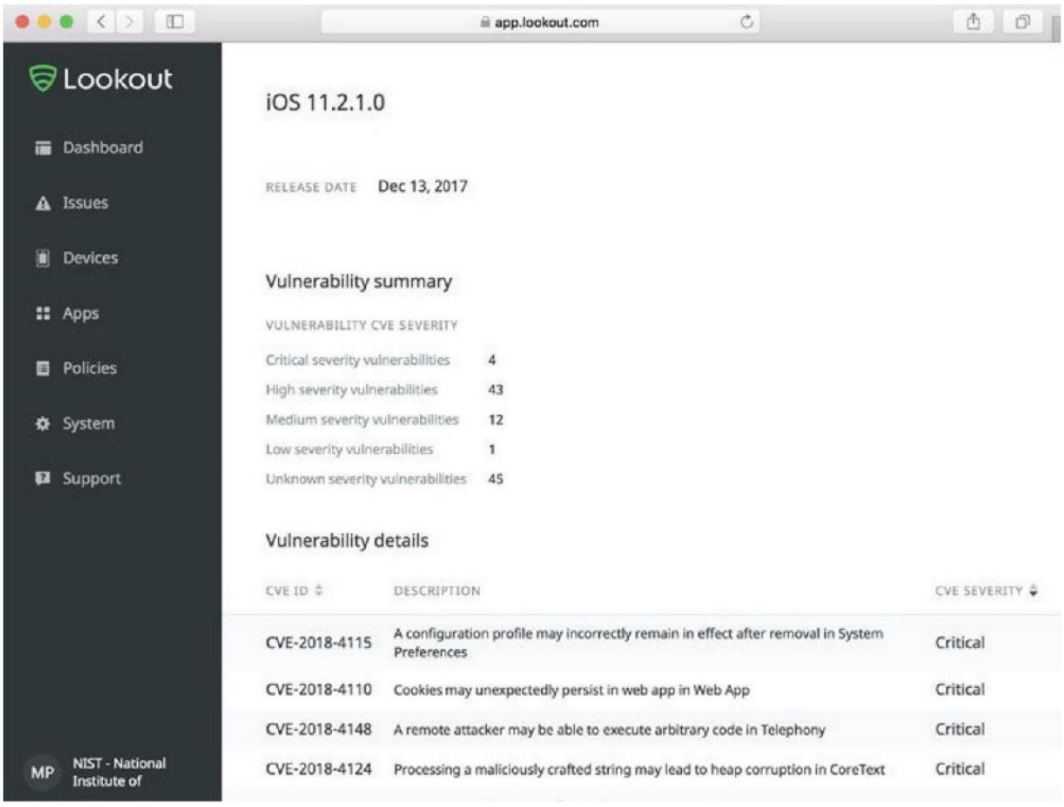


Rysunek H-10 Wykrycie włączonej opcji nieznanych źródeł

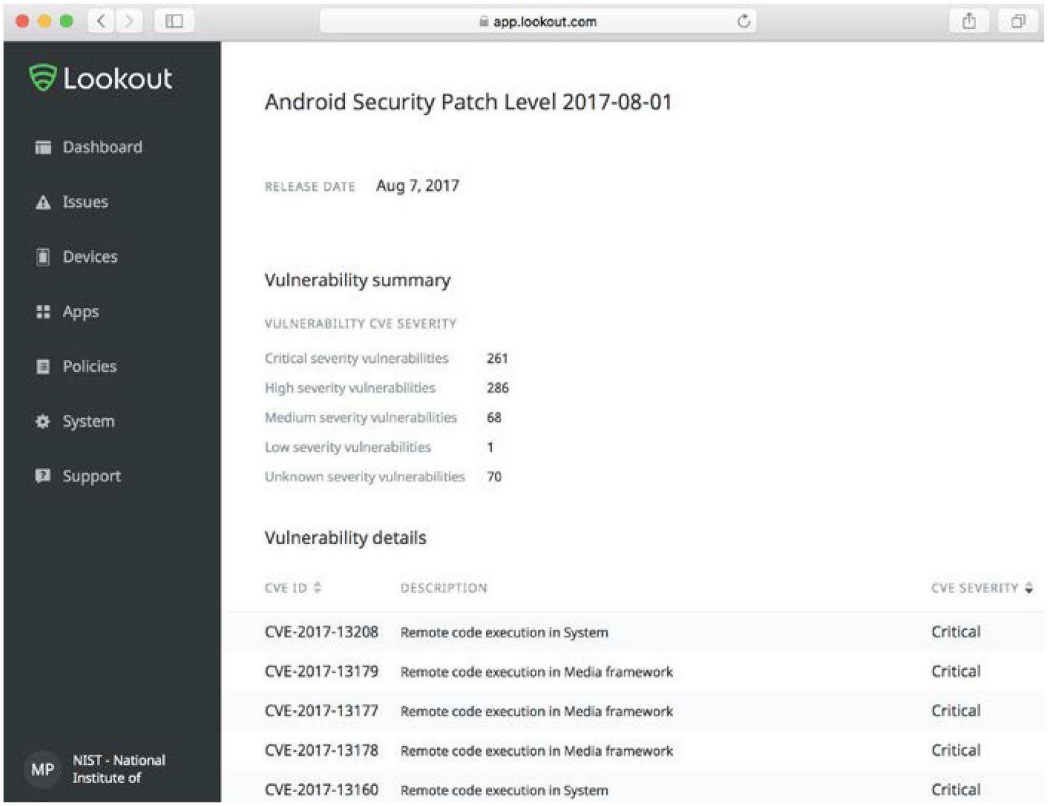
Tłumaczenie

H.4 ZDARZENIE POWODUJĄCE ZAGROŻENIE 4 — UTRATA POUFNOŚCI I INTEGRALNOŚCI W WYNIKU WYKORZYSTANIA ZNANEJ PODATNOŚCI W SYSTEMIE OPERACYJNYM LUB OPROGRAMOWANIU UKŁADOWYM

Na rysunku H-11 przedstawiono działanie funkcji usługi Lookout do identyfikowania znanych podatności w urządzeniach z systemami iOS i Android w nieaktualnych wersjach. Na rysunku H-12 zaprezentowano poziom poprawek zainstalowanych na urządzeniu.



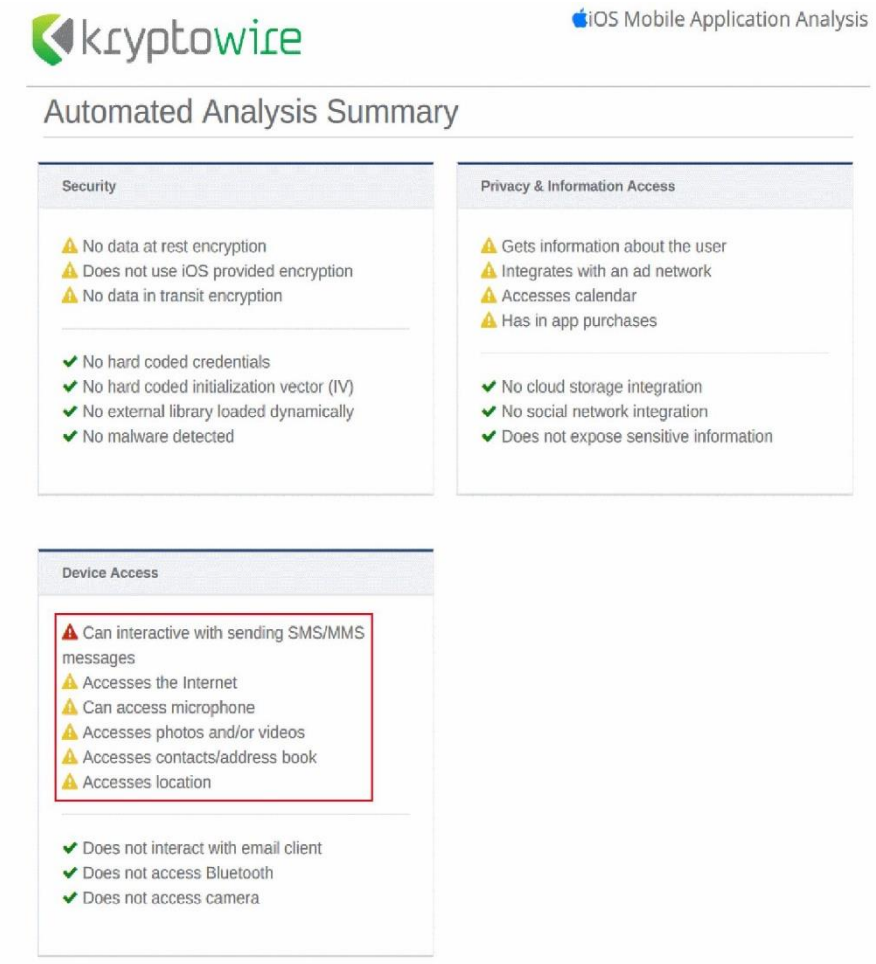
Rysunek H-11 Identyfikacja podatności



Rysunek H-12 Ekran poziomu zainstalowanych poprawek

H.5 ZDARZENIE POWODUJĄCE ZAGROŻENIE 5 — NARUSZENIE PRYWATNOŚCI POPRZEZ NIEWŁAŚCIWE WYKORZYSTANIE CZUJNIKÓW URZĄDZENIA

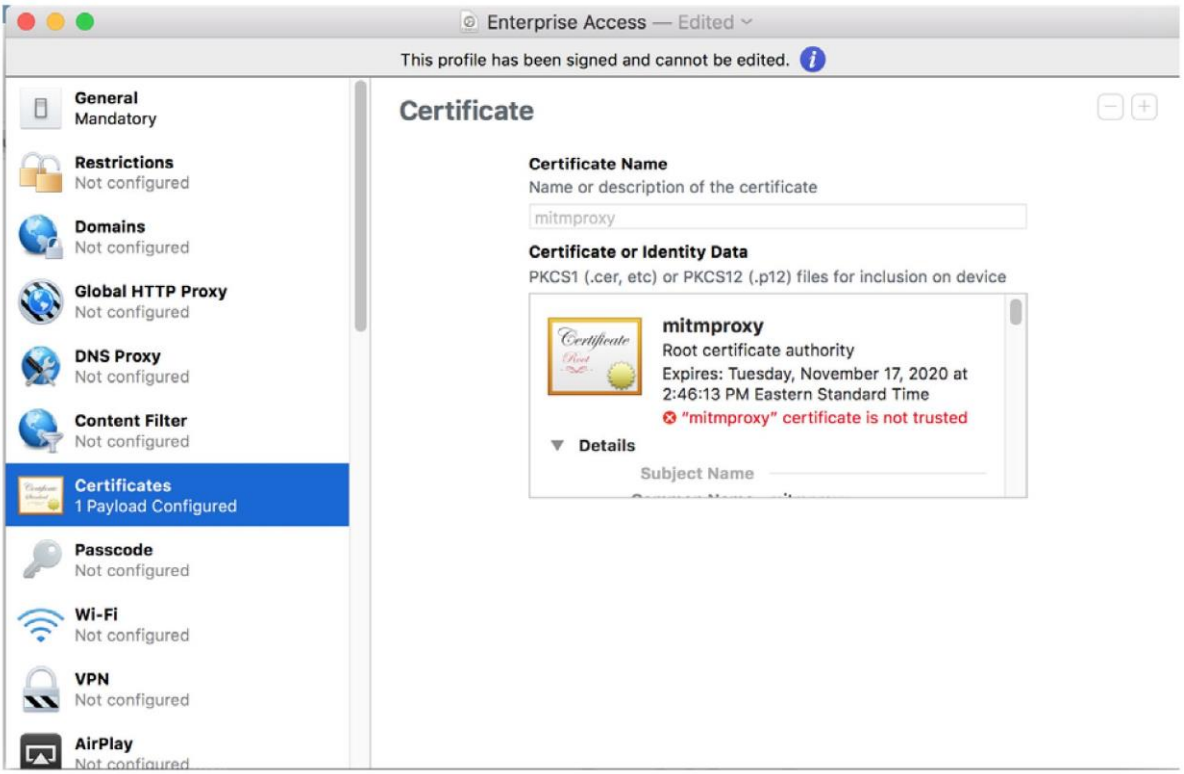
Na poniższym zrzucie ekranu przedstawiono raport z analizy aplikacji usługi Kryptowire z informacjami o uprawnieniach, których zażądała ta aplikacja.



Rysunek H-13 Raport z analizy usługi Kryptowire

H.6 ZDARZENIE POWODUJĄCE ZAGROŻENIE 6 — NARUSZENIE INTEGRALNOŚCI URZĄDZENIA LUB JEGO KOMUNIKACJI SIECIOWEJ POPRZEZ INSTALACJĘ ZŁOŚLIWEGO SYSTEMU EMM/MDM, SIECI, PROFILI VPN LUB CERTYFIKATÓW.

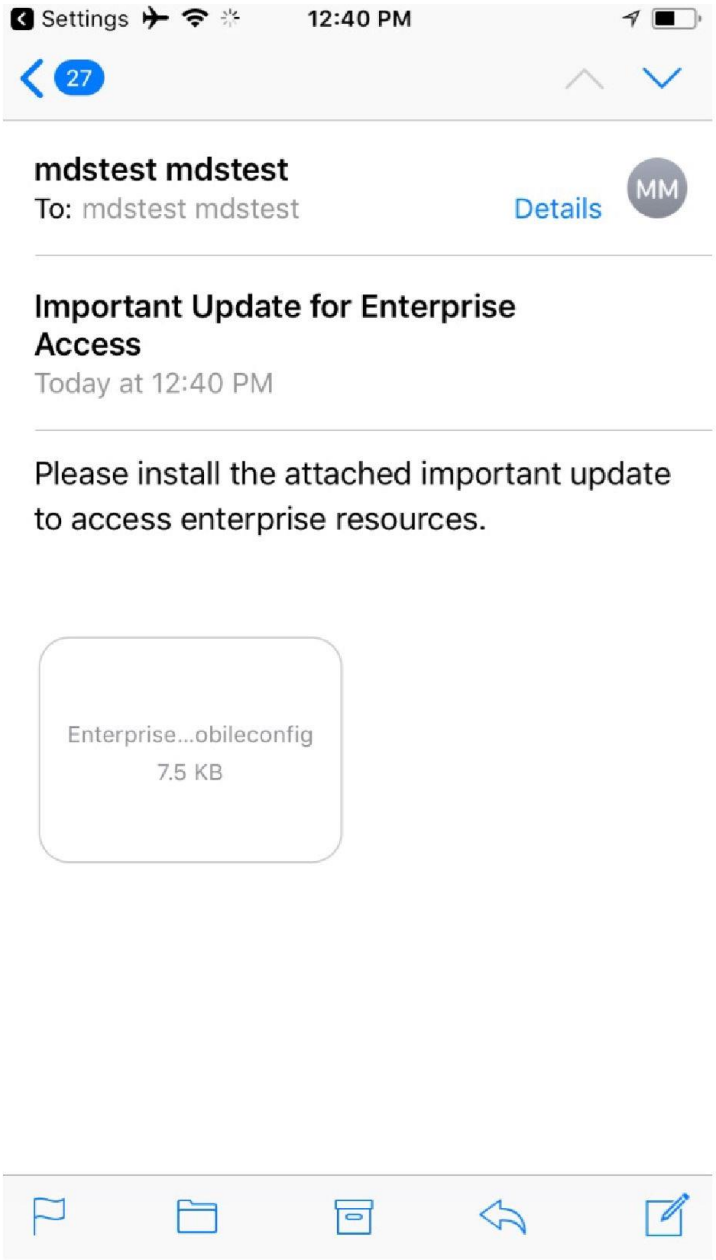
Na rysunku H-14 przedstawiono profil konfiguracji używany do konfigurowania i testowania zdarzenia powodującego zagrożenie nr 6.



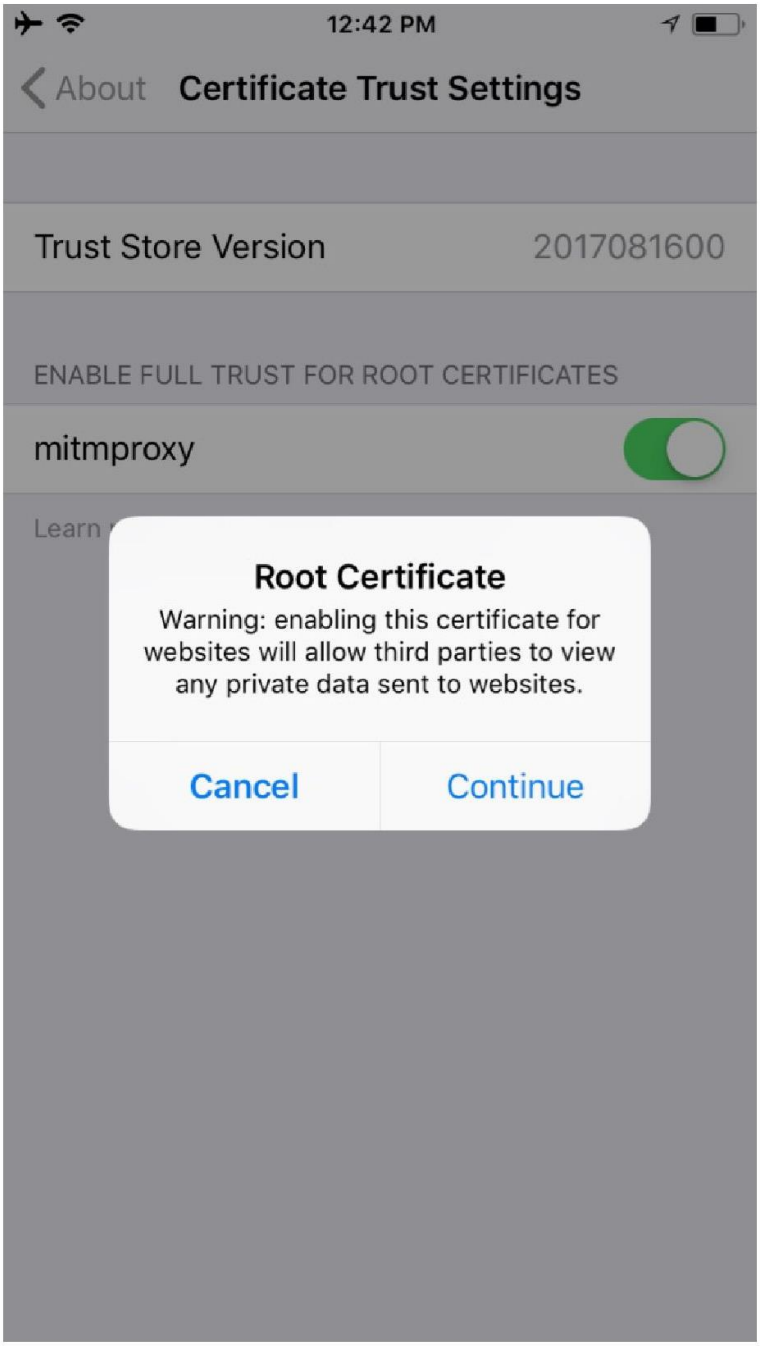
Rysunek H-14 Przykład profilu konfiguracji

Tłumaczenie

Rysunek H-15 przedstawia wiadomość e-mail zawierającą złośliwy profil konfiguracji urządzenia, a rysunek H-16 pokazuje ostrzeżenie wyświetlane użytkownikowi podczas próby oznaczenia złośliwego certyfikatu jako zaufanego roota.

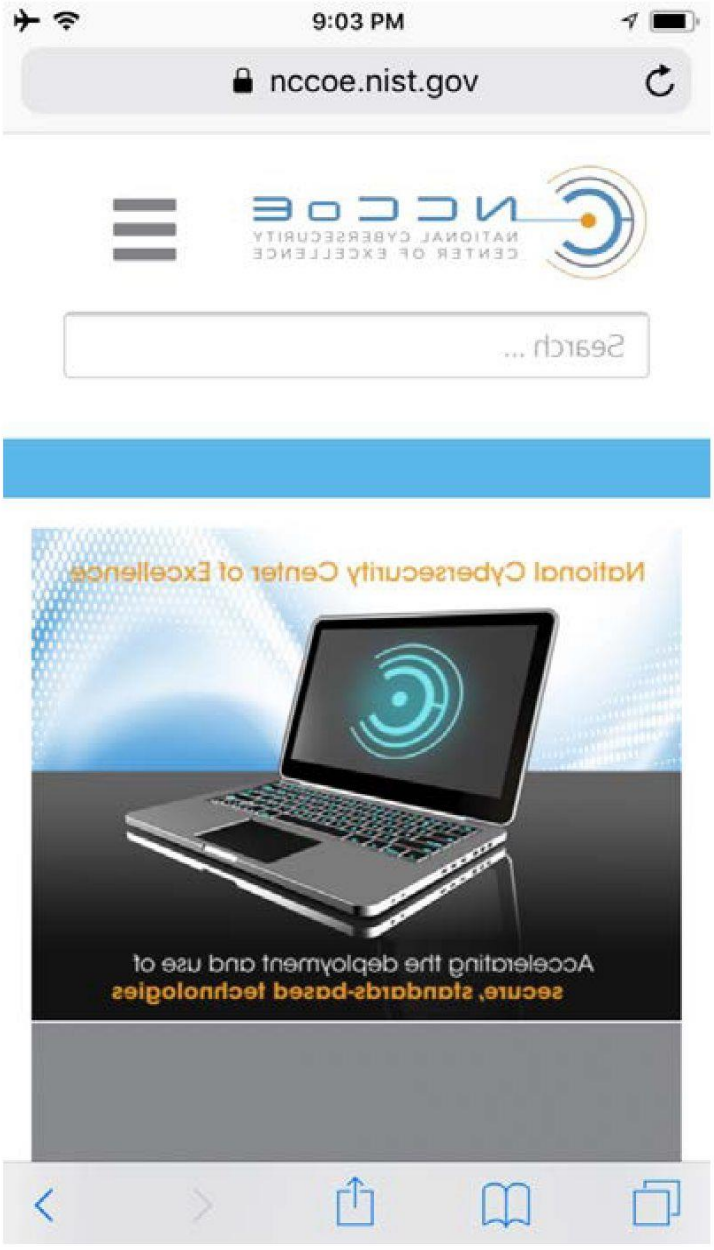


Rysunek H-15 Wiadomość e-mail z próbą wyłudzenia informacji przez profil konfiguracji



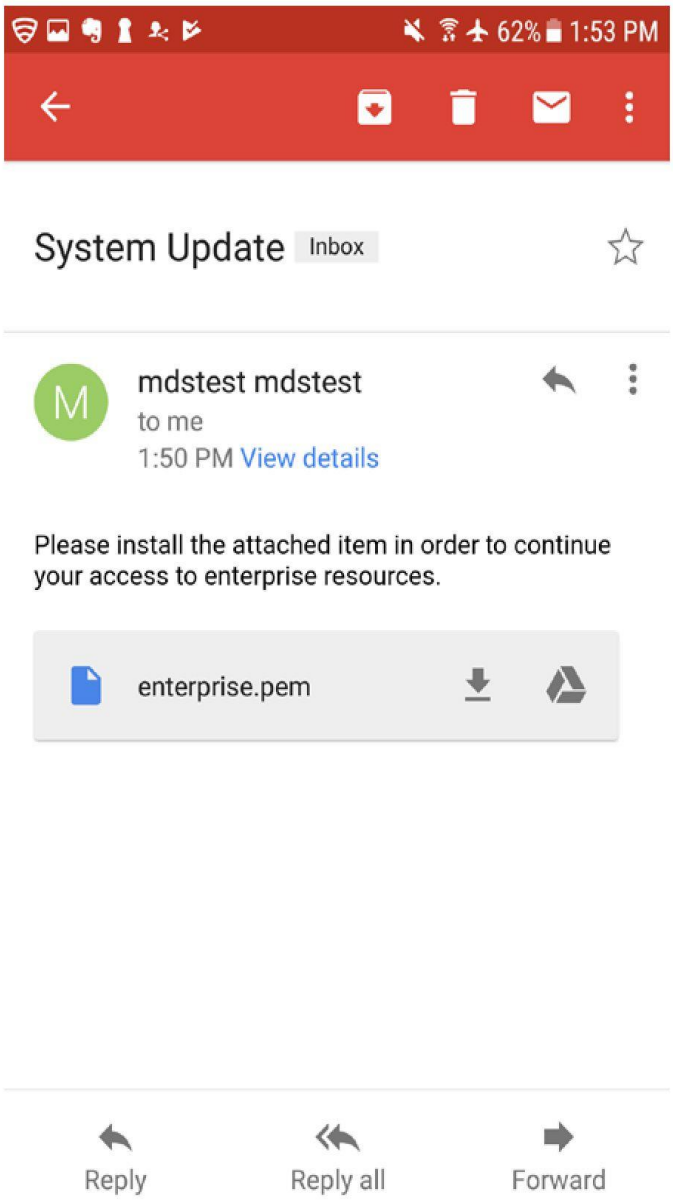
Rysunek H-16 Ostrzeżenie o włączeniu uprawnień certyfikatu głównego

Należy przejść do strony https z urządzenia mobilnego i sprawdzić, czy jej zawartość została odwrócona. Na rysunku H-17 widać, że atak typu „*person-in-the-middle*" na połączenie zabezpieczone protokołem TLS powiódł się.

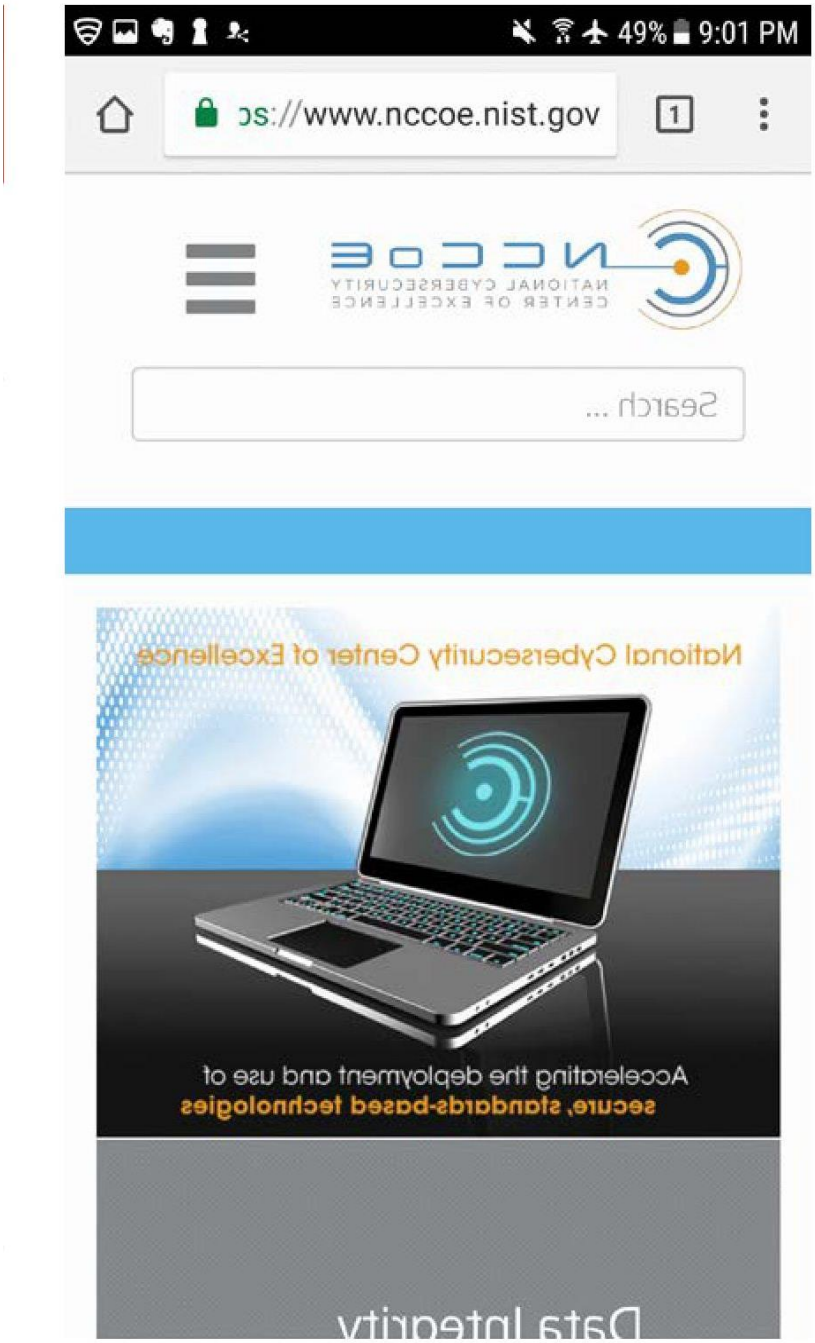


Rysunek H-17 Odwrócona strona internetowa

Na poniższych zrzutach ekranu przedstawiono atak typu „*person-in-the-middle*” na systemie Android.

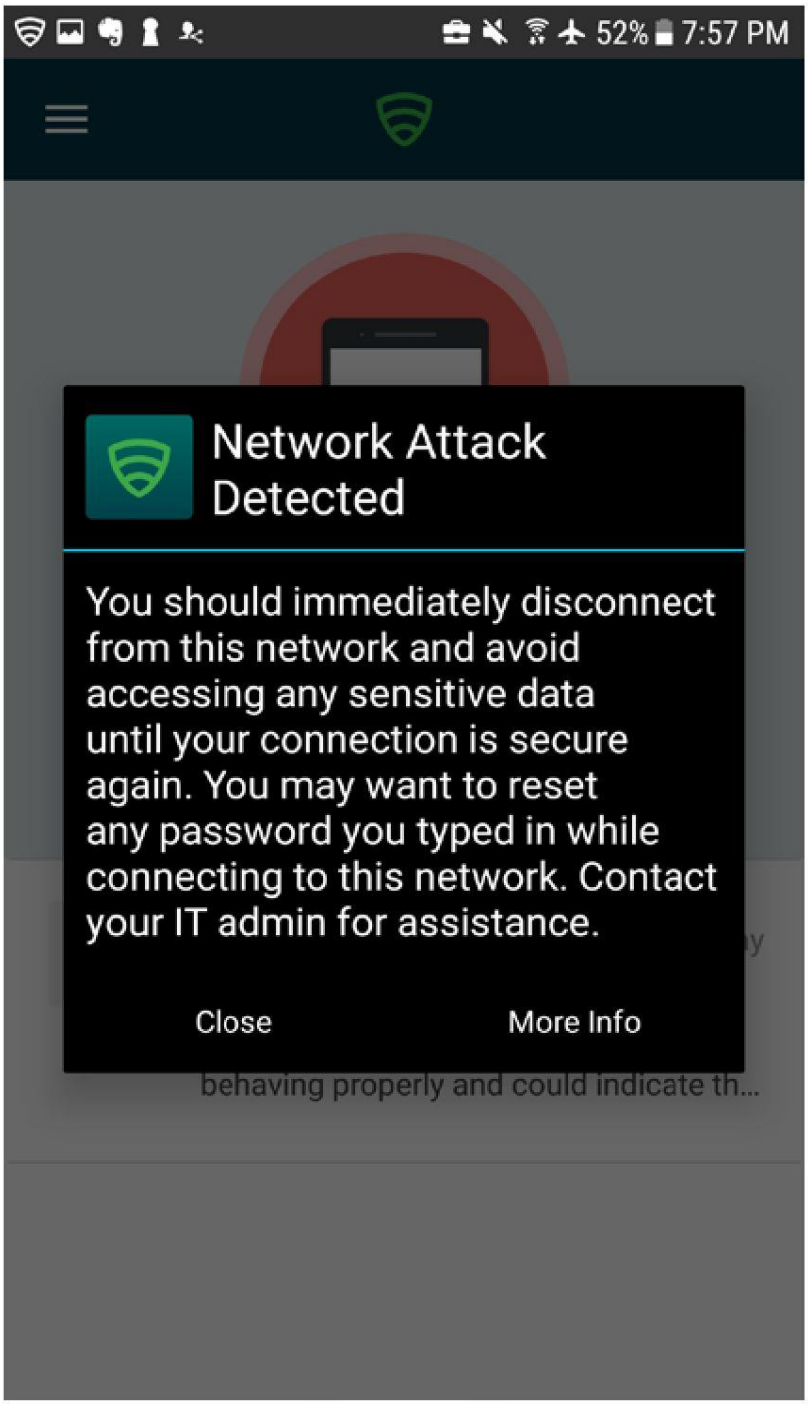


Rysunek H-18 Wiadomość e-mail z próbą wyłudzenia informacji przy użyciu certyfikatu



Rysunek H-19 Odwrócona strona internetowa

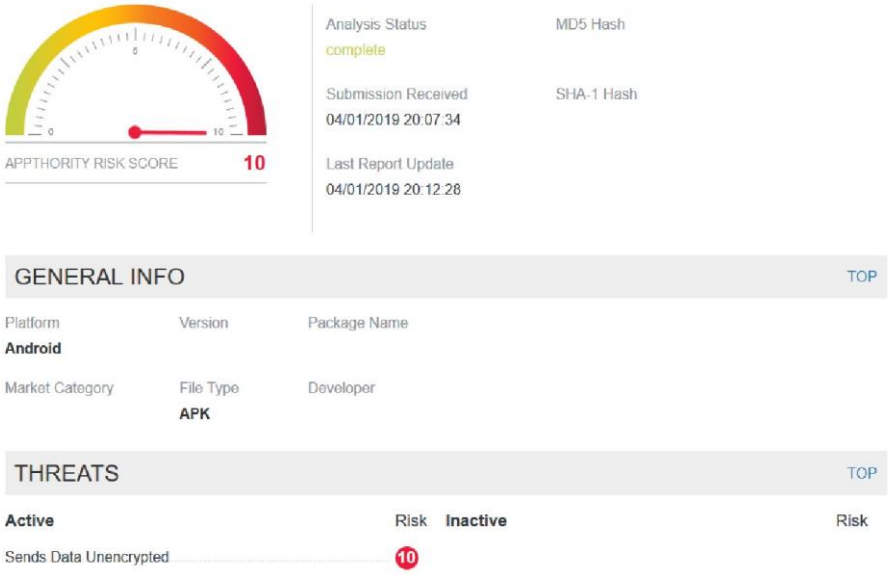
Atak typu „*person-in-the-middle*” jest wykrywany przez usługę Lookout, jak pokazano na rysunku H-20.



Rysunek H-20 Wykrycie ataku sieciowego

H.7 ZDARZENIE POWODUJĄCE ZAGROŻENIE 7 — UTRATA POUFNOŚCI WRAŻLIWYCH INFORMACJI POPRZEZ PODSŁUCHIWANIE NIEZASZYFROWANEJ KOMUNIKACJI URZĄDZENIA

Na poniższym zrzucie ekranu widać, jak usługa Appthority wykrywa aplikację wysyłającą niezaszyfrowane dane.

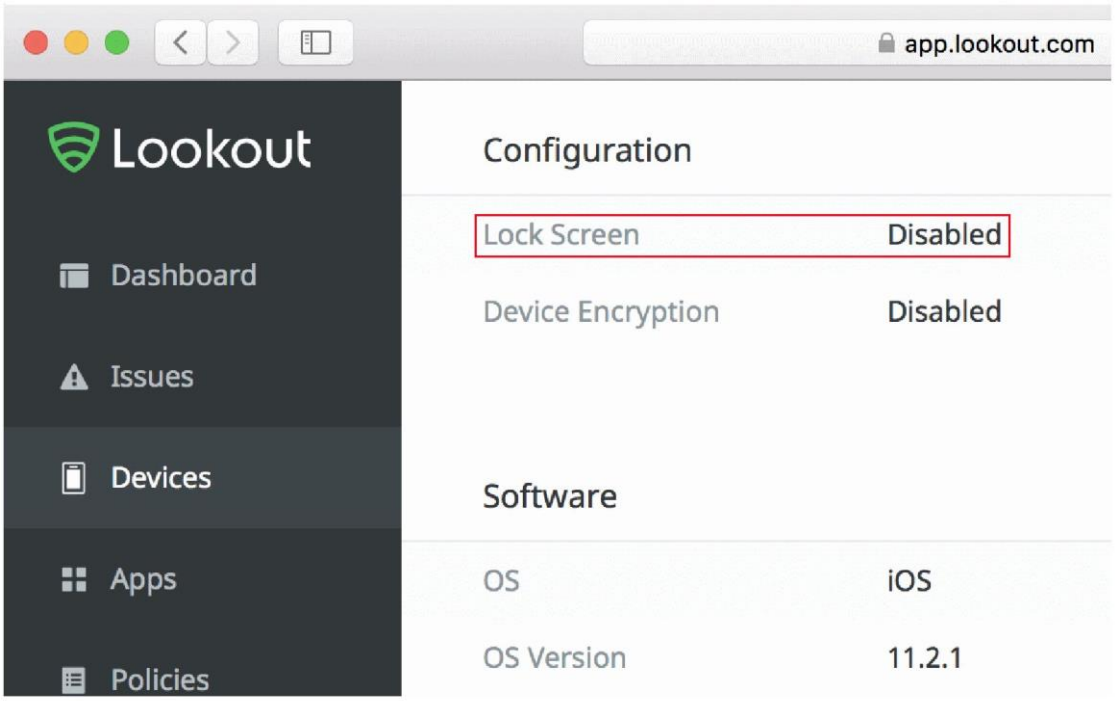


Rysunek H-21 Przesyłanie niezaszyfrowanych danych

Tłumaczenie

H.8 ZDARZENIE POWODUJĄCE ZAGROŻENIE 8 — NARUSZENIE INTEGRALNOŚCI URZĄDZENIA POPRZEZ ZASTOSOWANIE KODU ODBLOKOWUJĄCEGO, KTÓRY ZOSTAŁ ZAOBSERWOWANY, WYWNIOSKOWANY LUB POZYSKANY NA DRODZE ATAKU SIŁOWEGO

System MobileIron wdraża zasady na urządzeniach, aby wymusić obowiązkowe wprowadzanie osobistego numeru identyfikacyjnego i możliwość czyszczenia pamięci urządzenia. Usługa Lookout zgłasza urządzenia z wyłączonym ekranem blokady.

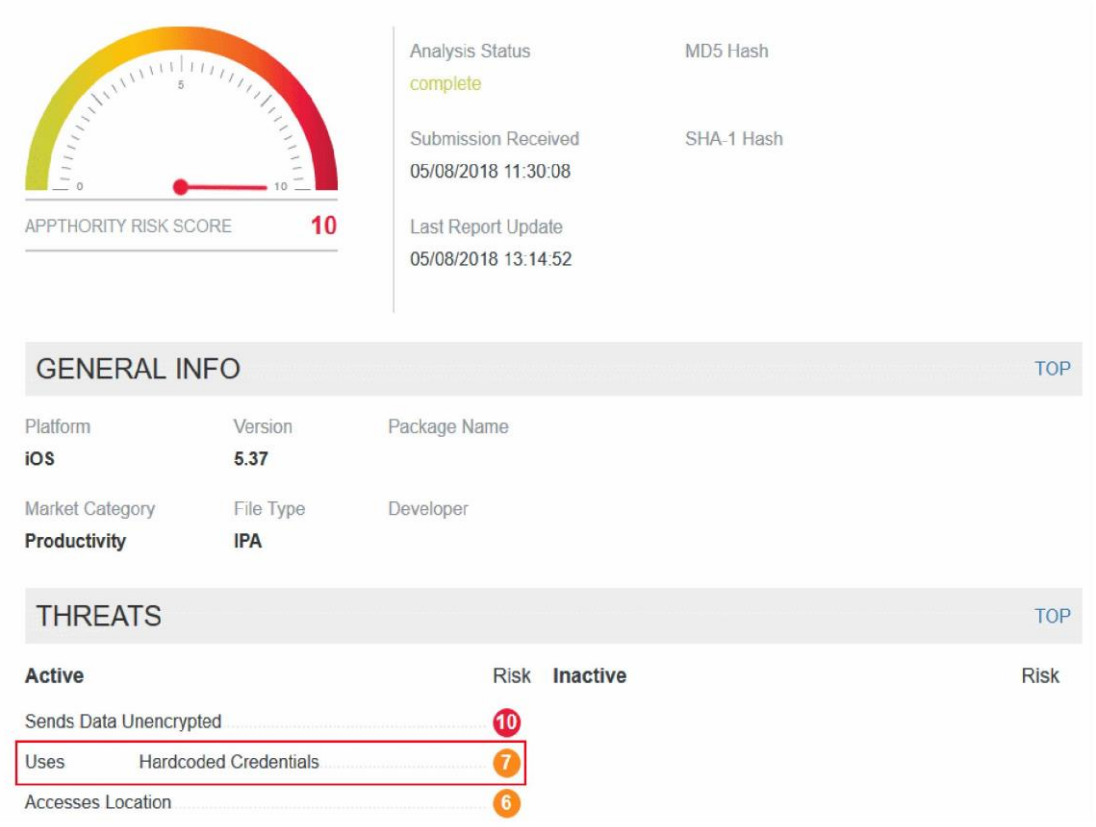


Rysunek H-22 Powiadomienie o wykryciu wyłączonego ekranu blokady

Tłumaczenie

H.9 ZDARZENIE POWODUJĄCE ZAGROŻENIE 9 — NIEAUTORYZOWANY DOSTĘP DO USŁUG ZAPLECZA POPRZEZ LUKI W UWIERZYTELNIANIU LUB PRZECHOWYWANIU DANYCH UWIERZYTELNIAJĄCYCH W WEWNĘTRZNIE OPRACOWANYCH APLIKACJACH

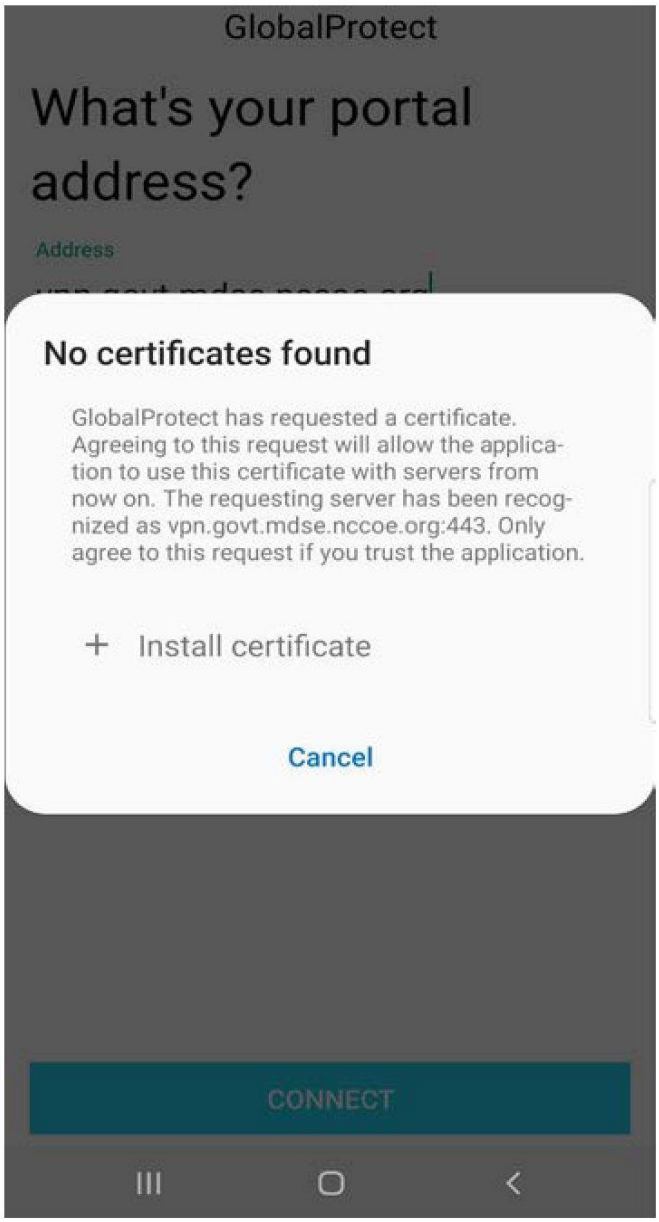
Jak widać na rysunku H-23, usługa Appthority wykryła, że aplikacja korzystała z danych uwierzytelniających znajdujących się w jej kodzie źródłowym. Korzystanie z danych uwierzytelniających zapisanych w kodzie aplikacji może stanowić podatność, jeśli zostaną one wykorzystane do uzyskania dostępu do zasobów przedsiębiorstwa przez nieautoryzowane podmioty lub do nieautoryzowanych działań.



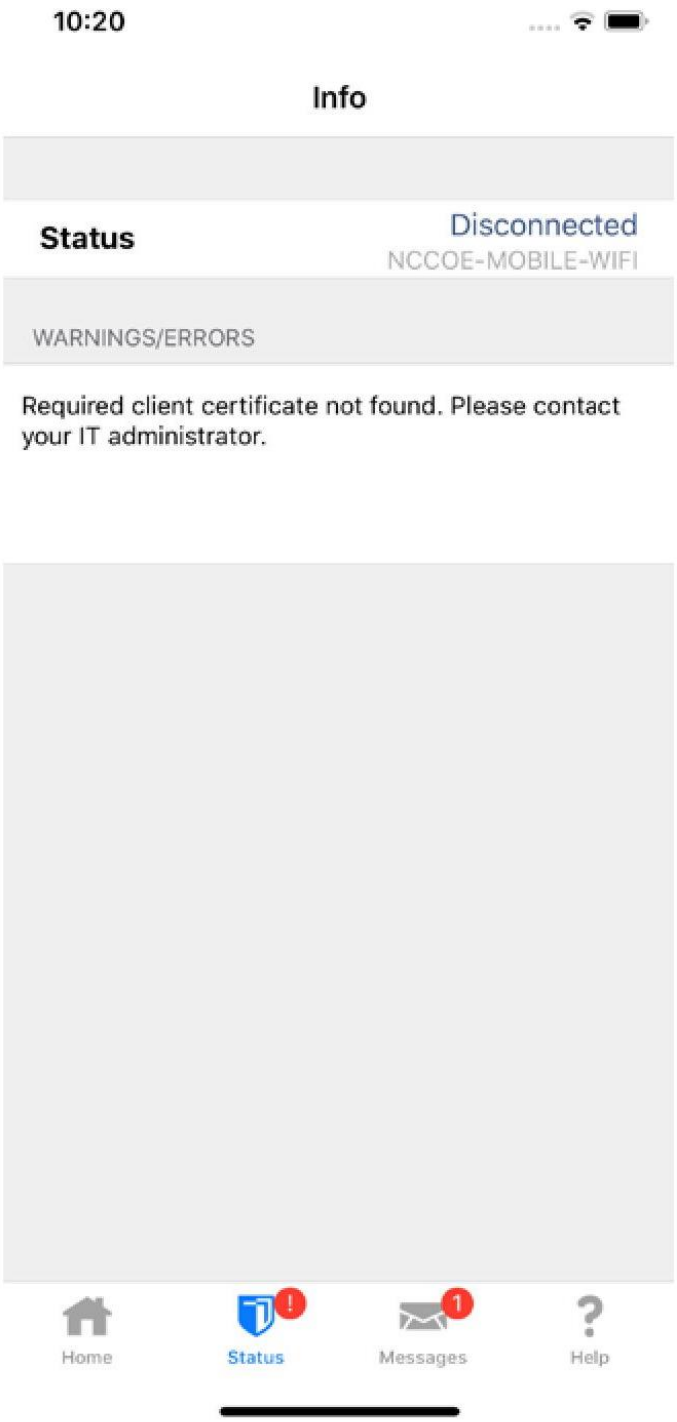
Rysunek H-23 Dane uwierzytelniające w kodzie aplikacji

H.10 ZDARZENIE POWODUJĄCE ZAGROŻENIE 10 — NIEAUTORYZOWANY DOSTĘP DO ZASOBÓW PRZEDSIĘBIORSTWA Z URZĄDZENIA NIEZARZĄDZANEGO I NARAŻONEGO NA NARUSZENIE BEZPIECZEŃSTWA

Na poniższych dwóch zrzutach ekranu przedstawiono brak możliwości połączenia się z siecią GlobalProtect VPN bez odpowiednich certyfikatów klienta, które można uzyskać tylko poprzez zarejestrowanie urządzenia w systemie MobileIron.



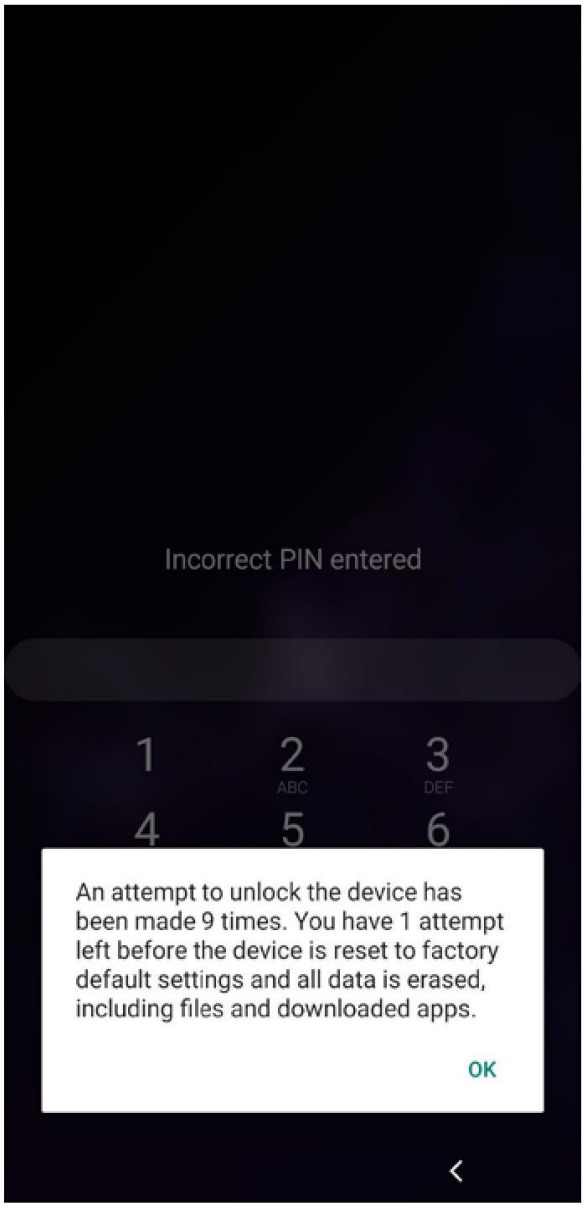
Rysunek H-24 Komunikat o braku certyfikatów w systemie Android



Rysunek H-25 Komunikat o braku certyfikatów w systemie iOS

H.11 ZDARZENIE POWODUJĄCE ZAGROŻENIE 11 — UTRATA DANYCH ORGANIZACJI Z POWODU ZGUBIENIA LUB KRADZIEŻY URZĄDZENIA

Na poniższym zrzucie ekranu widać ostatnie ostrzeżenie przed przywróceniem urządzenia do ustawień fabrycznych. w przypadku kradzieży urządzenia. Wszystkie dane firmowe zostałyby usunięte z urządzenia po jeszcze jednej nieudanej próbie odblokowania, udaremniając osiągnięcie celu przez złośliwy podmiot.



Rysunek H-26 Ostrzeżenie o wyczyszczeniu pamięci urządzenia w systemie Android

H.12 ZDARZENIE POWODUJĄCE ZAGROŻENIE 12 — UTRATA POUFNOŚCI DANYCH ORGANIZACJI Z POWODU ICH NIEAUTORYZOWANEGO PRZECHOWYWANIA W USŁUGACH NIEZARZĄDZANYCH PRZEZ ORGANIZACJĘ

Na poniższym zrzucie ekranu zaprezentowano jedną z opcji konfiguracji służącej zapobieganiu utracie danych w systemie MobileIron dla iOS.

Rysunek H-27 Uniemożliwianie wykonywania zrzutów ekranu i nagrywania ekranu

ZAŁĄCZNIK I PRZYKŁADOWE ZESTAWIENIE ŚRODKÓW BEZPIECZEŃSTWA

Tabela I-1 zawiera listę technologii wykorzystanych w tym projekcie i stanowi zestawienie ogólnych terminów dotyczących zastosowania, konkretnego użytego produktu, środków bezpieczeństwa zapewnianych przez produkt oraz odniesienie do odpowiedniej publikacji specjalnej (SP) Narodowego Instytutu Standaryzacji i Technologii (NIST) 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Work Roles*.

Od lewej do prawej, w kolumnach tabeli opisano:

- **Konkretny zastosowany produkt:** produkt od dostawcy wykorzystany w przykładowym rozwiązaniu.
- **Sposób działania komponentu w projekcie:** możliwości zapewniane przez komponent w przykładowym rozwiązaniu. Jest to zestawione z ogólnym terminem dotyczącym komponentu technologii mobilnej.
- **Odpowiednie podkategorie ram cyberbezpieczeństwa:** odpowiednie podkategorie ram cyberbezpieczeństwa, które komponent wprowadza do przykładowego rozwiązania.
- **Odpowiednie środki bezpieczeństwa zalecane przez NIST:** środki bezpieczeństwa zalecane w publikacji NIST SP 800-53 w wersji 4, które zostały zastosowane w przykładowym rozwiązaniu.
- **ISO/IEC 27001:2013:** zestawienie z zaleceniami normy 27001:2013 Międzynarodowej Organizacji Normalizacyjnej (ISO), Międzynarodowej Komisji Elektrotechnicznej (IEC), z którymi zgodność zapewnia komponent w przykładowym rozwiązaniu.
- **CIS 6:** środki bezpieczeństwa zalecane w publikacji Center for Internet Security (CIS) w wersji 6, które komponent zapewnia w przykładowym rozwiązaniu.
- **NIST SP 800-181,** *NICE Framework Work Roles:* Role robocze z ram NICE, które można wykorzystać do zarządzania korzystaniem z tego komponentu w przykładowym rozwiązaniu. W kolumnie tej znajdują się informacje na temat pracowników, którzy byliby zaangażowani we wsparcie tej części przykładowego rozwiązania.

Tabela I-1 Zestawienie standardów cyberbezpieczeństwa i najlepszych praktyk wykorzystanych w przykładowym rozwiązaniu

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
Analiza zagrożeń urządzeń mobilnych						
Appthority Cloud Service	Analiza zagrożeń urządzeń mobilnych	ID.RA-1 — Podatności aktywów są identyfikowane i dokumentowane	Ocena bezpieczeństwa i autoryzacja CA2, CA-7, CA-8 Szacowanie ryzyka RA-3, RA-5 Zakup systemów i usług SA-5, SA-11 Integralność systemu i informacji SI-2, SI-4, SI-5	A.12.6.1 Kontrola podatności technicznych A.18.2.3 Przegląd zgodności technicznej	CSC 4 Ciągła ocena podatności i usuwanie jej skutków	SP-RSK-002 Oceniający środki bezpieczeństwa SP-ARC-002 Architekt bezpieczeństwa informacji OM-ANA-001 Analityk bezpieczeństwa systemów PR-VAM-001 Analityk ds. oceny podatności PR-CDA-001 Analityk ds. cyberobrony OV-MGT-001

Tłumaczenie

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
						Menedżer ds. bezpieczeństwa systemów informatycznych
		ID.RA-3 — Zagrożenia, zarówno wewnętrzne, jak i zewnętrzne, są identyfikowane i dokumentowane	Szacowanie ryzyka RA-3 Integralność systemów i informacji SI-5 Program przeciwdziałania zagrożeniom wewnętrznym PM-12, PM-16	Punkt 6.1.2 Proces szacowania ryzyka związanego z informacjami	CSC 4 Ciągła ocena podatności i usuwanie jej skutków	SP-RSK-002 Oceniający środki bezpieczeństwa PR-CDA-001 Analityk ds. cyberobrony OV-SPP-001 Specjalista i menedżer ds. pracowników cyberbezpieczeństwa OV-TEA-001 Osoba opracowująca program nauczania w zakresie cyberbezpieczeństwa AN-TWA-001 Analityk ds. zagrożeń/ostrzeżeń

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
						PR-VAM-001 Analityk ds. oceny podatności OV-MGT-001 Menedżer ds. bezpieczeństwa systemów informacyjnych
		DE.CM-4 — Wykryto złośliwy kod	Integralność systemów i informacji SI-3, SI-8	A.12.2.1 Środki bezpieczeństwa chroniące przed złośliwym oprogramowaniem	CSC 4 Ciągła ocena podatności i usuwanie jej skutków CSC 7 Zabezpieczenia poczty elektronicznej i przeglądarki internetowej CSC 8 Zabezpieczenia przed złośliwym oprogramowaniem	PR-VAM-001 Analityk ds. oceny podatności PR-CIR-001 Osoba reagująca na incydenty z zakresu cyberobrony PR-CDA-001 Analityk ds. cyberobrony OM-NET-001 Specjalista ds. operacji sieciowych

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
					CSC 12 Ochrona granic	
		DE.CM-5 — Wykryto nieautoryzowany kod mobilny	Kod mobilny SC18, SC-44 Integralność systemów i informacji SI-4	A.12.5.1 Instalacja oprogramowania w systemach operacyjnych A.12.6.2 Ograniczenia dotyczące instalacji oprogramowania	CSC 7 Zabezpieczenia poczty elektronicznej i przeglądarki internetowej CSC 8 Zabezpieczenia przed złośliwym oprogramowaniem	PR-CDA-001 Analityk ds. cyberobrony OM-NET-001 Specjalista ds. operacji sieciowych
Usługa weryfikacji aplikacji mobilnych						
Kryptowire Cloud Service	Weryfikacja aplikacji	ID.RA-1 — Podatności aktywów są identyfikowane i dokumentowane	Ocena bezpieczeństwa i autoryzacja CA-2, CA-7, CA-8 Szacowanie ryzyka RA-3, RA-5 Pozyskiwanie systemów i usług	A.12.6.1 Kontrola podatności technicznych A.18.2.3 Przegląd zgodności technicznej	CSC 4 Ciągła ocena podatności i usuwanie jej skutków	SP-RSK-002 Oceniający środki bezpieczeństwa SP-ARC-002 Architekt bezpieczeństwa informacji OM-ANA-001 Analityk bezpieczeństwa

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
			SA-5, SA-11 Integralność systemu i informacji SI-2, SI-4, SI-5			systemów PR-VAM-001 Analityk ds. oceny podatności PR-CDA-001 Analityk ds. cyberobrony OV-MGT-001 Menedżer ds. bezpieczeństwa systemów informacyjnych
		ID.RA-3 — Zagrożenia, zarówno wewnętrzne, jak i zewnętrzne, są identyfikowane i dokumentowane	Szacowanie ryzyka RA-3 Integralność systemów i informacji SI-5 Program przeciwdziałania zagrożeniom wewnętrznym PM-12, PM-16	Punkt 6.1.2 Proces szacowania ryzyka związanego z informacjami	CSC 4 Ciągła ocena podatności i usuwanie jej skutków	SP-RSK-002 Oceniający środki bezpieczeństwa OM-ANA-001 Analityk bezpieczeństwa systemów OV-SPP-001

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
						Specjalista i menedżer ds. pracowników cyberbezpieczeństwa OV-TEA-001 Osoba opracowująca program nauczania w zakresie cyberbezpieczeństwa AN-TWA-001 Analityk ds. zagrożeń/ostrzeżeń PR-VAM-001 Analityk ds. oceny podatności PR-CDA-001 Analityk ds. cyberobrony OV-MGT-001 Menedżer ds. bezpieczeństwa systemów informatycznych

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
		DE.CM-4 — Wykryto złośliwy kod	Integralność systemów i informacji SI-3, SI-8	A.12.2.1 Środki bezpieczeństwa chroniące przed złośliwym oprogramowaniem	CSC 4 Ciągła ocena podatności i usuwanie jej skutków CSC 7 Zabezpieczenia poczty elektronicznej i przeglądarki internetowej CSC 8 Zabezpieczenia przed złośliwym oprogramowaniem CSC 12 Ochrona granic	PR-CIR-001 Osoba reagująca na incydenty z zakresu cyberobrony PR-CDA-001 Analityk ds. cyberobrony PR-VAM-001 Analityk ds. oceny podatności OM-NET-001 Specjalista ds. operacji sieciowych
		DE.CM-5 — Wykryto nieautoryzowany kod mobilny	Kod mobilny SC18, SC-44 Integralność systemów i informacji SI-4	A.12.5.1 Instalacja oprogramowania w systemach operacyjnych	CSC 7 Zabezpieczenia poczty elektronicznej i przeglądarki internetowej CSC 8	PR-CDA-001 Analityk ds. cyberobrony OM-NET-001 Specjalista ds. operacji sieciowych

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
				A.12.6.2 Ograniczenia dotyczące instalacji oprogramowania	Zabezpieczenia przed złośliwym oprogramowaniem	
Obrona przed zagrożeniami urządzeń mobilnych						
Lookout Cloud Service/Lookout Agent w wersji 5.10.0.142 (iOS), 5.9.0.420 (Android)	Ochrona przed zagrożeniami mobilnymi/ bezpieczeństwo punktów końcowych w Internecie	PR.AC-5 — Integralność sieci jest chroniona (np. segregacja sieci, segmentacja sieci).	Kontrola dostępu AC4, AC-10 Ochrona systemu i komunikacji SC-7	A.13.1.1 Sieciowe środki bezpieczeństwa A.13.1.3 Segregacja w sieciach A.13.2.1 Zasady i procedury przesyłania informacji A.14.1.2 Zabezpieczanie usług aplikacji w sieciach publicznych A.14.1.3 Ochrona transakcji usług aplikacji	CSC 9 Ograniczanie i kontrola portów, protokołów i usług sieciowych CSC 14 Kontrolowany dostęp oparty na zasadzie wiedzy koniecznej CSC 15 Kontrola dostępu bezprzewodowego CSC 18 Bezpieczeństwo oprogramowania (aplikacji)	OM-ADM-001 Administrator systemu OV-SPP-002 Planista ds. polityk i strategii cyberbezpieczeństwa PR-CDA-001 Analityk ds. cyberobrony OM-NET-001 Specjalista ds. operacji sieciowych

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
		PR.PT-4 — Sieci komunikacyjne i kontrolne są chronione	Kontrola dostępu AC-4, AC-17, AC-18 Polityka i procedury planowania awaryjnego CP-8 Ochrona systemu i komunikacji SC-7, SC-19, SC-20, SC21, SC-22, SC-23, SC-24, SC-25, S.C.-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	A.13.1.1 Sieciowe środki bezpieczeństwa A.13.1.3 Segregacja w sieciach A.14.1.3 Ochrona transakcji usług aplikacji	CSC 8 Zabezpieczenia przed złośliwym oprogramowaniem CSC 12 Ochrona granic systemu CSC 15 Kontrola dostępu bezprzewodowego	OM-ADM-001 Administrator systemu OV-SPP-002 Planista ds. polityk i strategii cyberbezpieczeństwa OV-MGT-002 Menedżer ds. bezpieczeństwa komunikacji (COMSEC) SP-ARC-0001 Architekt infrastruktury przedsiębiorstwa PR-CDA-001 Analityk ds. cyberobrony SP-ARC-002 Architekt bezpieczeństwa informacji OM-NET-001 Specjalista ds. operacji sieciowych

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
		DE.CM-5 — Wykryto nieautoryzowany kod mobilny	Kod mobilny SC-18, SC-44 Integralność systemów i informacji SI-4	A.12.5.1 Instalacja oprogramowania w systemach operacyjnych A.12.6.2 Ograniczenia dotyczące instalacji oprogramowania	CSC 7 Zabezpieczenia poczty elektronicznej i przeglądarki internetowej CSC 8 Zabezpieczenia przed złośliwym oprogramowaniem	PR-CDA-001 Analityk ds. cyberobrony OM-NET-001 Specjalista ds. operacji sieciowych
Zarządzanie mobilnością w przedsiębiorstwie						
MobileIron Core, wersja 9.7.0.1	Zarządzanie mobilnością w przedsiębiorstwie	ID.AM-1 — Fizyczne urządzenia i systemy w organizacji są inwentaryzowane	Inwentaryzacja komponentów systemu informacyjnego CM-8 Inwentaryzacja systemu informatycznego PM-5	A.8.1.1 Inwentaryzacja aktywów A.8.1.2 Własność aktywów	CSC 1 Inwentaryzacja autoryzowanych i nieautoryzowanych urządzeń	OM-STS-001 Specjalista ds. wsparcia technicznego OM-ADM-001 Administrator systemu

Tłumaczenie

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
		PR.AC-1 — Tożsamości i dane uwierzytelniające są wydawane, zarządzane, weryfikowane, odwoływane i audytowane dla autoryzowanych urządzeń, użytkowników i procesów	Kontrola dostępu AC1, AC-2 Identyfikacja i uwierzytelnianie IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	A.9.2.1 Rejestracja i wyrejestrowywanie użytkowników A.9.2.2 Udzielanie dostępu użytkownikom A.9.2.3 Zarządzanie uprawnieniami dostępu uprzywilejowanego A.9.2.4 Zarządzanie niejawnymi informacjami uwierzytelniającymi użytkowników A.9.2.6 Usuwanie lub dostosowywanie uprawnień dostępu A.9.3.1 Korzystanie z niejawnych informacji	CSC 1 Inwentaryzacja autoryzowanych i nieautoryzowanych urządzeń CSC 5 Kontrolowane korzystanie z uprawnień administracyjnych CSC 15 Kontrola dostępu bezprzewodowego CSC 16 Monitorowanie i kontrola kont	OV-SPP-002 Planista ds. polityk i strategii cyberbezpieczeństwa OM-ADM-001 Administrator systemu OV-MGT-002 Menedżer ds. bezpieczeństwa komunikacji (COMSEC) OM-STS-001 Specjalista ds. wsparcia technicznego OM-ANA-001 Analityk bezpieczeństwa systemów PR-CDA-001 Analityk ds. cyberobrony

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
				uwierzytelniających A.9.4.2 Procedury bezpiecznego logowania A.9.4.3 System zarządzania hasłami		
		PR.AC-6 — Tożsamości są weryfikowane i powiązane z danymi uwierzytelniającymi oraz potwierdzane w interakcjach.	Kontrola dostępu AC1, AC-2, AC-3, AC-16, AC-19, AC-24 Identyfikacja i uwierzytelnianie IA-1, IA-2, IA-4, IA-5, IA-8 Ochrona fizyczna i środowiskowa PE-2 Bezpieczeństwo osobowe PS-3	A.7.1.1 Kontrola pracowników A.9.2.1 Rejestracja i wyrejestrowywanie użytkowników	CSC 16 Monitorowanie i kontrola kont	OV-SPP-002 Planista ds. polityk i strategii cyberbezpieczeństwa OV-MGT-002 Menedżer ds. bezpieczeństwa komunikacji (COMSEC) OM-ADM-001 Administrator systemu

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
		PR.IP-1 — Tworzona i utrzymywana jest podstawowa konfiguracja technologii informacyjnej/ przemysłowych systemów kontroli, uwzględniająca zasady bezpieczeństwa (np. zasadę minimalnej funkcjonalności)	Inwentaryzacja komponentów systemu informacyjnego CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9 Pozyskiwanie systemów i usług SA-10	A.12.1.2 Zarządzanie zmianą A.12.5.1 Instalacja oprogramowania w systemach operacyjnych A.12.6.2 Ograniczenia dotyczące instalacji oprogramowania A.14.2.2 Procedury kontroli zmian w systemie A.14.2.3 Przegląd techniczny aplikacji po zmianie platformy operacyjnej A.14.2.4	CSC 3 Bezpieczne konfiguracje sprzętu i oprogramowania na urządzeniach mobilnych, laptopach, stacjach roboczych i serwerach CSC 9 Ograniczanie i kontrola portów, protokołów i usług sieciowych CSC 11 Bezpieczne konfiguracje urządzeń sieciowych, takich jak zapory, routery i przełączniki	SP-ARC-002 Architekt bezpieczeństwa informacji OV-SPP-002 Planista ds. polityk i strategii cyberbezpieczeństwa SP-SYS-001 Specjalista ds. bezpieczeństwa systemów informatycznych OM-ADM-001 Administrator systemu PR-VAM-001 Analityk ds. oceny podatności OM-NET-001 Specjalista ds. operacji sieciowych

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
				Ograniczenia dotyczące zmian w pakietach oprogramowania		OV-MGT-001 Menedżer ds. bezpieczeństwa systemów informacyjnych OM-STS-001 Specjalista ds. wsparcia technicznego
MobileIron Agent w wersji 11.0.1A (iOS), 10.2.1.1.3R (Android)	EMM/agent w punkcie końcowym	PR.DS-6 — Mechanizmy kontroli integralności są wykorzystywane do weryfikacji aplikacji i układowego oprogramowania oraz integralności informacji	Ochrona systemu i komunikacji S.C.-1 Integralność systemów i informacji SI-7	A.12.2.1 Środki bezpieczeństwa chroniące przed złośliwym oprogramowaniem A.12.5.1 Instalacja oprogramowania w systemach operacyjnych A.14.1.2 Zabezpieczanie	CSC 2 Inwentaryzacja autoryzowanego i nieautoryzowanego oprogramowania CSC 3 Bezpieczne konfiguracje sprzętu i oprogramowania na urządzeniach mobilnych, laptopach, stacjach roboczych i serwerach	OV-SPP-002 Planista ds. polityk i strategii cyberbezpieczeństwa SP-ARC-0001 Architekt infrastruktury przedsiębiorstwa OV-MGT-001 Menedżer ds. bezpieczeństwa systemów informacyjnych OM-ADM-001 Administrator systemu

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
				usług aplikacji w sieciach publicznych A.14.1.3 Ochrona transakcji usług aplikacji A.14.2.4 Ograniczenia dotyczące zmian w pakietach oprogramowania		OM-STS-001 Specjalista ds. wsparcia technicznego
Zaufane środowisko wykonawcze						
Qualcomm (wersja zależna od urządzenia mobilnego)	Zaufane środowisko wykonawcze	PR.DS-1 — Przechowywane dane są chronione	Obniżanie klasyfikacji nośników MP8 Ochrona systemu i komunikacji SC-12, SC-28	A.8.2.3 Postępowanie z aktywami	CSC 13 Ochrona danych CSC 14 Kontrolowany dostęp oparty na zasadzie wiedzy koniecznej	OV-SPP-002 Planista ds. zasad i strategii cyberbezpieczeństwa PR-INF-001 Specjalista ds. wsparcia w zakresie infrastruktury cyberobronnej OV-LGA-002 Specjalista ds.

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
						prywatności/menedżer ds. zgodności z zasadami ochrony prywatności OV-MGT-002 Menedżer COMSEC OM-NET-001 Specjalista ds. operacji sieciowych OM-ANA-001 Analityk bezpieczeństwa systemów
		PR.DS-6 — Mechanizmy kontroli integralności są wykorzystywane do weryfikacji aplikacji i układowego oprogramowania oraz integralności informacji	Ochrona systemu i komunikacji SC-16 Integralność systemów i informacji SI-7	A.12.2.1 Środki bezpieczeństwa chroniące przed złośliwym oprogramowaniem A.12.5.1	CSC 2 Inwentaryzacja autoryzowanego i nieautoryzowanego oprogramowania	OV-SPP-002 Planista ds. zasad i strategii cyberbezpieczeństwa PR-CDA-001 Analityk ds. cyberobrony SP-ARC-0001 Architekt infrastruktury przedsiębiorstwa

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
				Instalacja oprogramowania w systemach operacyjnych A.14.1.2 Zabezpieczanie usług aplikacji w sieciach publicznych A.14.1.3 Ochrona transakcji usług aplikacji A.14.2.4 Ograniczenia dotyczące zmian w pakietach oprogramowania	CSC 3 Bezpieczne konfiguracje sprzętu i oprogramowania na urządzeniach mobilnych	OV-MGT-001 Menedżer ds. bezpieczeństwa systemów informacyjnych OM-STS-001 Specjalista ds. wsparcia technicznego OM-ADM-001 Administrator systemu
		PR.DS-8 — Mechanizmy kontroli integralności są wykorzystywane do	Specjalista ds. zarządzania konfiguracją SA10	A.11.2.4 Konserwacja sprzętu	Nie dotyczy	OM-ADM-001 Administrator systemu SP-ARC-0001

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
		weryfikacji integralności sprzętu	Integralność systemów i informacji SI-7			Architekt infrastruktury przedsiębiorstwa
		DE.CM-4 — Wykryto złośliwy kod	Integralność systemów i informacji SI-3, SI-8	A.12.2.1 Środki bezpieczeństwa chroniące przed złośliwym oprogramowaniem	CSC 5 Kontrolowane korzystanie z uprawnień administracyjnych CSC 7 Zabezpieczenia poczty elektronicznej i przeglądarki internetowej CSC 14 Kontrolowany dostęp oparty na zasadzie wiedzy koniecznej CSC 16 Monitorowanie i kontrola kont	PR-CDA-001 Analityk ds. cyberobrony PR-INF-001 Specjalista ds. wsparcia w zakresie infrastruktury cyberobronnej PR-VAM-001 Analityk ds. oceny podatności OM-NET-001 Specjalista ds. operacji sieciowych PR-CDA-001 Analityk ds. cyberobrony

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
Wirtualna sieć prywatna						
Palo Alto Networks, PA-220 Wersja 8.1.1	Wirtualna sieć prywatna	PR.AC-3 — Dostęp zdalny jest zarządzany	Kontrola dostępu AC1, AC-17, AC-19, AC-20 Ochrona systemu i komunikacji SC-15	A.6.2.1 Polityka dotycząca urządzeń mobilnych A.6.2.2 Praca zdalna A.11.2.6 Bezpieczeństwo sprzętu i aktywów poza siedzibą firmy A.13.1.1 Sieciowe środki bezpieczeństwa A.13.2.1 Zasady i procedury przesyłania informacji	CSC 12 Ochrona granic systemu	OV-SPP-002 Planista ds. zasad i strategii cyberbezpieczeństwa OV-MGT-002 Menedżer ds. bezpieczeństwa komunikacji (COMSEC) OM-NET-001 Specjalista ds. operacji sieciowych
		PR.AC-5 — Integralność sieci	Kontrola dostępu AC4, AC-10	A.13.1.1 Sieciowe środki	CSC 9 Ograniczanie i kontrola portów,	PR-CDA-001 Analityk ds. cyberobrony

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
		jest chroniona (np. segregacja sieci, segmentacja sieci).	Ochrona systemu i komunikacji SC-7	bezpieczeństwa A.13.1.3 Segregacja w sieciach A.13.2.1 Zasady i procedury przesyłania informacji A.14.1.2 Zabezpieczanie usług aplikacji w sieciach publicznych A.14.1.3 Ochrona transakcji usług aplikacji	protokołów i usług sieciowych CSC 14 Kontrolowany dostęp oparty na zasadzie wiedzy koniecznej CSC 15 Kontrola dostępu bezprzewodowego CSC 18 Bezpieczeństwo oprogramowania aplikacyjnego	OM-ADM-001 Administrator systemu OM-NET-001 Specjalista ds. operacji sieciowych
		PR.AC-6 — Tożsamości są weryfikowane i powiązane z danymi uwierzytelniającymi	Kontrola dostępu AC- 1, AC-2, AC-3, AC16, AC-19, AC-24	A.7.1.1 Kontrola pracowników A.9.2.1 Rejestracja i wyrejestrowywanie	CSC 16 Monitorowanie i kontrola kont	OV-SPP-002 Planista ds. zasad i strategii cyberbezpieczeństwa OV-MGT-002

Tłumaczenie

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
		oraz potwierdzane w interakcjach.	Identyfikacja i uwierzytelnianie IA-1, IA-2, IA-4, IA-5, IA-8 Ochrona fizyczna i środowiskowa PE-2, PS-3	użytkowników		Menedżer ds. bezpieczeństwa komunikacji (COMSEC) OM-ADM-001 Administrator systemu
		PR.DS-2 — Dane w trakcie przesyłania są chronione	Ochrona systemu i komunikacji SC-8, SC-11, SC-12	A.8.2.3 Postępowanie z aktywami A.13.1.1 Sieciowe środki bezpieczeństwa A.13.2.1 Zasady i procedury przesyłania informacji A.13.2.3 Wiadomości elektroniczne	CSC 13 Ochrona danych CSC 14 Kontrolowany dostęp oparty na zasadzie wiedzy koniecznej	OV-SPP-002 Planista ds. zasad i strategii cyberbezpieczeństwa OV-MGT-002 Menedżer ds. bezpieczeństwa komunikacji (COMSEC) OV-LGA-002 Specjalista ds. prywatności/menedżer ds. zgodności z zasadami ochrony prywatności OM-NET-001

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
				A.14.1.2 Zabezpieczanie usług aplikacji w sieciach publicznych A.14.1.3 Ochrona transakcji usług aplikacji		Specjalista ds. operacji sieciowych
		PR.PT-4 — Sieci komunikacyjne i kontrolne są chronione	Kontrola dostępu AC4, AC-17, AC-18 Planowanie awaryjne CP-8	A.13.1.1 Sieciowe środki bezpieczeństwa A.13.2.1 Zasady i procedury przesyłania informacji A.14.1.3 Ochrona transakcji usług aplikacji	CSC 8 Zabezpieczenia przed złośliwym oprogramowaniem CSC 12 Ochrona granic systemu CSC 15 Kontrola dostępu bezprzewodowego	PR-INF-001 Specjalista ds. wsparcia w zakresie infrastruktury cyberobronnej OV-SPP-002 Planista ds. zasad i strategii cyberbezpieczeństwa PR-CDA-001 Analityk ds. cyberobrony OM-NET-001 Specjalista ds. operacji sieciowych

Konkretny zastosowany produkt	Sposób działania komponentu w projekcie	Odpowiednie podkategorie z ram cyberbezpieczeństwa w wersji 1.1	Odpowiednie środki bezpieczeństwa zlecane w publikacji NIST SP 800-53 w wersji 4	ISO/IEC 27001:2013	CIS 6	Role robocze z NIST SP 800-181, NICE Framework Work Roles
			Ochrona systemu i komunikacji SC-7, SC-19, SC-20, SC21, SC-22, SC-23, SC-24, SC-25, SC29, SC-32, SC-36, SC-37, SC-38, SC39, SC-40, SC-41, SC-43			

26 września 2024

Bezpieczeństwo urządzeń mobilnych: Organizacyjne urządzenia mobilne obsługiwane osobiście przez użytkowników *(COPE)*

Tom C
Poradniki „How-to”

NIST SPECIAL PUBLICATION 1800-21C

Mobile Device Security:
Corporate-Owned Personally-Enabled (COPE)

Volume C:
How-to Guides

Joshua M. Franklin*
Gema Howell
Kaitlin Boeckl
Naomi Lefkovitz
Ellen Nadeau*
Applied Cybersecurity Division
Information Technology Laboratory

Dr. Behnam Shariati
University of Maryland, Baltimore County
Department of Computer Science and Electrical Engineering
Baltimore, Maryland

Jason G. Ajmo
Christopher J. Brown
Spike E. Dog
Frank Javar
Michael Peck
Kenneth F. Sandlin
The MITRE Corporation
McLean, Virginia

Former employee; all work for this publication done while at employer

September 2020

Final

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-21

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Partnerzy / podmioty współpracujące w zakresie technologii, które uczestniczyły w tym projekcie, przedstawiły swoje możliwości w odpowiedzi na ogłoszenie w rejestrze federalnym. Respondenci dysponujący odpowiednimi możliwościami lub produktami zostali zaproszeni do podpisania umowy o współpracy w zakresie badań i rozwoju (*ang. Cooperative Research and Development Agreement – CRADA*) z NIST, umożliwiającej im udział w konsorcjum w celu zbudowania tego przykładowego rozwiązania. Współpracowaliśmy z:

Partner / podmiot współpracujący w zakresie technologii	**Zakres udziału**
Appthority*	Appthority Cloud Service, Mobile Threat Intelligence
Kryptowire	Kryptowire Cloud Service, Application Vetting
Lookout	Lookout Cloud Service/Lookout Agent w wersji 5.10.0.142 (iOS), 5.9.0.420 (Android), Mobile Threat Defense
MobileIron	MobileIron Core w wersji 9.7.0.1, MobileIron Agent w wersji 11.0.1A (iOS), 10.2.1.1.3R (Android), Enterprise Mobility Management
Palo Alto Networks	Palo Alto Networks PA-220
Qualcomm	Qualcomm Trusted Execution Environment (wersja zależy od urządzenia)

* Appthority (firma przejęta przez Symantec – oddział Broadcom).

1. WPROWADZENIE

W kolejnych tomach niniejszego przewodnika pokazujemy specjalistom ds. technologii informatycznych i inżynierom bezpieczeństwa, w jaki sposób wdrożyliśmy przykładowe rozwiązanie. Omawiamy wszystkie produkty zabezpieczające urządzenia mobilne zastosowane w niniejszym projekcie referencyjnym. Nie powielamy dokumentacji od twórców produktów, która powinna być powszechnie dostępna. W tomach tych pokazujemy, w jaki sposób połączyliśmy produkty w naszym środowisku.

Uwaga: Nie są to wyczerpujące samouczki. Istnieje wiele możliwych konfiguracji usług i zabezpieczeń dla tych produktów, które wykraczają poza zakres tego projektu referencyjnego.

1.1. STRUKTURA PRZEWODNIKA PO PRAKTYKACH

W niniejszym przewodniku Narodowego Instytutu Standaryzacji i Technologii (*ang. National Institute of Standards and Technology – NIST*) dotyczącym cyberbezpieczeństwa przedstawiono projekt referencyjny oparty na standardach i zapewniający użytkownikom informacje potrzebne do sprostania wyzwaniom związanym z wdrażaniem systemu bezpieczeństwa urządzeń mobilnych (*ang. Mobile Device Security – MDS*) dla organizacyjnych urządzeń mobilnych obsługiwanych osobiście przez użytkowników (*ang. Corporate-Owned Personally-Enabled – COPE*). Ten projekt referencyjny jest modułowy i może być wdrażany w całości lub w części.

Niniejszy przewodnik obejmuje trzy tomy:

- NIST SP 1800-21A: *Streszczenie*
- NIST SP 1800-21B: *Podejście, architektura i charakterystyka bezpieczeństwa* — co zbudowaliśmy i dlaczego
- NIST SP 1800-21C: *Poradniki* „How-to” — instrukcje dotyczące tworzenia przykładowego rozwiązania **(jesteś tutaj)**

W zależności od roli pełnionej w organizacji, z niniejszego przewodnika można korzystać na różne sposoby:

Osoby podejmujące decyzje biznesowe, w tym kluczowy personel ds. bezpieczeństwa i technologii, będą zainteresowani streszczeniem, NIST SP 1800-21A, w którym poruszono następujące tematy:

- wyzwania stojące przed przedsiębiorstwami związane z bezpiecznym wdrażaniem urządzeń mobilnych COPE,
- przykładowe rozwiązanie zaprojektowane w krajowym centrum doskonałości w dziedzinie bezpieczeństwa (*ang. National Cybersecurity Center of Excellence — NCCoE*),
- korzyści z wdrożenia przykładowego rozwiązania.

Menedżerowie ds. technologii lub programów bezpieczeństwa, którzy są zainteresowani tym, jak identyfikować, rozumieć, oceniać i ograniczać ryzyko, będą zainteresowani publikacją *NIST SP 1800-21B*, w której opisano, co zrobiliśmy i dlaczego. Szczególnie pomocne będą dla nich poniższe punkty:

- Punkt 3.4, „Szacowanie ryzyka", zawiera opis przeprowadzonej przez nas analizy ryzyka.
- Punkt 4.3, „Zestawienie środków bezpieczeństwa", zawiera porównanie charakterystyki bezpieczeństwa tego przykładowego rozwiązania ze standardami cyberbezpieczeństwa i najlepszymi praktykami.

Publikację *Executive Summary*, NIST SP 1800-21A, można udostępnić członkom zespołu kierowniczego, aby pomóc im zrozumieć znaczenie przyjmowania rozwiązań opartych na standardach przy rozwiązywaniu problemów związanych z wdrażaniem zabezpieczeń urządzeń mobilnych COPE.

Specjaliści IT, którzy chcą wdrożyć takie podejście, uznają cały przewodnik za przydatny. Mogą oni skorzystać z części zawierającej poradnik How-to, NIST SP 1800-21C, aby odtworzyć całość lub część rozwiązania stworzonego w naszym laboratorium. Niniejsza część dokumentu zawierająca poradnik obejmuje szczegółowe instrukcje dotyczące instalowania, konfigurowania i integrowania produktów w celu wdrożenia przykładowego rozwiązania. Nie powielamy dokumentacji od twórców

produktów, która jest powszechnie dostępna. Pokazujemy, w jaki sposób włączyliśmy produkty do naszego środowiska, aby stworzyć przykładowe rozwiązanie.

W niniejszym przewodniku założono, że specjaliści ds. technologii informacyjnych mają doświadczenie we wdrażaniu produktów związanych z bezpieczeństwem w przedsiębiorstwie. W celu sprostania wyzwaniu wykorzystaliśmy szereg produktów komercyjnych, jednak niniejszy przewodnik nie ma na celu promowania tych konkretnych produktów. Dana organizacja może przyjąć to rozwiązanie lub takie, które jest zgodne z tymi wytycznymi w całości, lub można użyć tego przewodnika jako punktu wyjścia do dostosowania i wdrożenia części przykładowego rozwiązania z tego przewodnika do lokalnego zarządzania bezpieczeństwem urządzeń mobilnych. Eksperci ds. bezpieczeństwa w danej organizacji powinni określić, które produkty najlepiej zintegrują się z istniejącymi narzędziami i infrastrukturą systemu IT. Mamy nadzieję, że użytkownicy będą poszukiwać produktów zgodnych z obowiązującymi standardami i najlepszymi praktykami. Punkt 3.6, „Technologie", zawiera listę produktów, z których korzystaliśmy, a w załączniku I powiązano je ze środkami cyberbezpieczeństwa stosowanymi w ramach opisywanego rozwiązania referencyjnego.

W przewodniku NIST po praktykach w zakresie cyberbezpieczeństwa nie opisano ostatecznego rozwiązania problemu, ale możliwe rozwiązanie. Komentarze, sugestie i historie pomyślnego wdrożenia umożliwią ulepszenie kolejnych wersji niniejszego przewodnika. Prosimy o przesyłanie swoich opinii na adres mobile-nccoe@nist.gov.

1.2. OMÓWIENIE ROZWIĄZANIA

Gdy pracownicy muszą być w ciągłym ruchu, urządzenia mobilne mogą służyć jako urządzenia tymczasowo zastępujące stacje robocze. Ich zaletą jest wygoda użytkowania, przenośność i funkcjonalność. Jednak pod wieloma względami urządzenia mobilne różnią się od zwykłych komputerowych stacji roboczych, a do zabezpieczenia ich interakcji z przedsiębiorstwem wymagane są alternatywne narzędzia do zarządzania. Aby sprostać temu wyzwaniu z zakresu bezpieczeństwa, NCCoE podjęło współpracę z partnerami w ramach swojej społeczności oraz zbudowało zespół, który opracował rzeczywisty scenariusz wdrożenia urządzeń

mobilnych w przedsiębiorstwie. W ramach tego scenariusza przedstawiono szereg wyzwań związanych z bezpieczeństwem, które mogą pojawić się w przedsiębiorstwie podczas wdrażania urządzeń mobilnych.

Środowisko laboratoryjne wykorzystane do opracowania tego rozwiązania obejmuje komponenty architektoniczne, funkcje i najlepsze praktyki oparte na standardach, które opisano w tomie B. Partnerzy zespołu projektowego dostarczyli technologie zabezpieczeń wykorzystane do wdrożenia komponentów architektury i funkcji. W odniesieniu do technologii bezpieczeństwa stosowane są najlepsze praktyki oparte na standardach, aby zapewnić wprowadzenie odpowiednich środków bezpieczeństwa w celu sprostania wyzwaniom przedstawionym w opracowanym scenariuszu.

W niniejszym punkcie przewodnika udokumentowano proces budowy i omówiono konkretne konfiguracje używane do opracowania bezpiecznego wdrożenia urządzeń mobilnych.

***Uwaga:* System Android for Work (AFW) został przemianowany na Android Enterprise. W momencie pisania tego dokumentu nosił on nazwę Android for Work.**

1.3. KONWENCJE TYPOGRAFICZNE

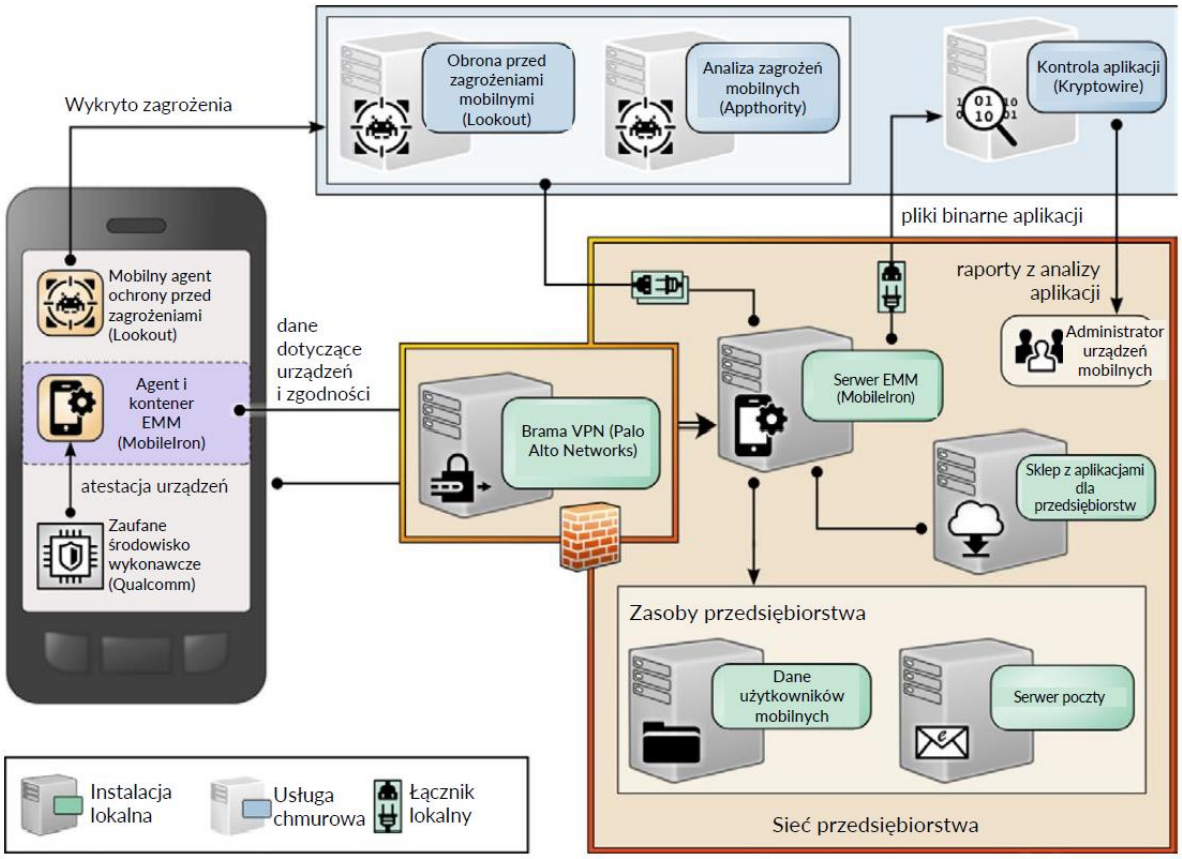
W poniższej tabeli przedstawiono konwencje typograficzne stosowane w niniejszym tomie.

Tabela 1-1 Konwencje typograficzne

Krój pisma/symbol	Znaczenie	Przykład
Kursywa	nazwy plików i nazwy ścieżek; odniesienia do dokumentów, które nie są hiperłączami; nowe terminy; symbole zastępcze	Szczegółowe definicje terminów można znaleźć w Glosariuszu NCCoE.
Pogrubienie	nazwy menu, opcji, przycisków poleceń i pól	Wybierz **File** (Plik) > **Edit** (Edytuj).
Czcionka o stałej szerokości znaków	dane wejściowe wiersza poleceń, dane wyjściowe komputera na ekranie, przykładowy kod i kody stanu	mkdir
Pogrubiona czcionka o stałej szerokości znaków	dane wprowadzane przez użytkownika w wierszu poleceń zestawione z danymi wyjściowymi komputera	service sshd start
niebieski tekst	łącze do innej części dokumentu, adres URL strony internetowej lub adres e-mail	Wszystkie publikacje NCCoE (NIST) są dostępne pod adresem https://www.nccoe.nist.gov.

1.4. PODSUMOWANIE ARCHITEKTURY LOGICZNEJ

Na poniższej grafice zilustrowano główne komponenty tej przykładowej implementacji i przedstawiono sposób ich interakcji.



Rysunek 1-1 Podsumowanie architektury logicznej

2. INSTRUKCJE INSTALOWANIA PRODUKTÓW

Niniejszy punkt przewodnika zawiera szczegółowe instrukcje dotyczące instalowania i konfigurowania kluczowych produktów wykorzystywanych w architekturze przedstawionej poniżej.

W naszym środowisku laboratoryjnym przykładowe rozwiązanie było logicznie oddzielone wirtualną siecią lokalną (*ang. Virtual Local Area Network – VLAN*) — każda sieć VLAN reprezentowała oddzielne środowisko fikcyjnego przedsiębiorstwa. Granice sieci dla tej przykładowej implementacji zostały wprowadzone przez sieć VPN / zaporę sieciową Palo Alto Networks. W ich ramach utrzymywane są trzy strefy: po jednej dla Internetu / rozległej sieci komputerowej (*ang. Wide Area Network – WAN*), strefy zdemilitaryzowanej (*ang. Demilitarized Zone – DMZ*) i organizacyjnej sieci lokalnej (*ang. Local Area Network – LAN*).

2.1. MOBILE THREAT DETECTION FIRMY APPTHORITY

Firma Appthority udostępniła testową wersję swojej usługi Mobile Threat Detection. W celu utworzenia instancji usługi dla swojej organizacji należy skontaktować się z firmą Appthority (Symantec) (https://www.symantec.com/).

2.2. EMM+S FIRMY KRYPTOWIRE

Firma Kryptowire udostępniła testową wersję swojej usługi weryfikacji aplikacji EMM+S. W celu utworzenia instancji usługi dla swojej organizacji należy skontaktować się z firmą Kryptowire (https://www.kryptowire.com/mobile-app-security/).

2.3. MOBILE ENDPOINT SECURITY FIRMY LOOKOUT

Firma Lookout udostępniła testową wersję swojej usługi Mobile Endpoint Security (MES). W celu utworzenia instancji usługi dla swojej organizacji należy skontaktować się z firmą Lookout (https://www.lookout.com/products/mobile-endpoint-security).

2.4. MOBILEIRON CORE FIRMY MOBILERON

System MobileIron Core jest kluczowym produktem w pakiecie MobileIron. W poniższych punktach opisano poszczególne etapy jego instalowania, konfigurowania i integrowania z usługą Active Directory (AD).

2.4.1. INSTALOWANIE SYSTEMU MOBILEIRON CORE I STAND-ALONE SENTRY

Aby zainstalować system MobileIron Core, należy wykonać poniższe kroki:

1. Pobierz z portalu pomocy technicznej MobileIron kopię przewodnika instalowania aplikacji *On-Premise Installation Guide for MobileIron Core*, *Sentry*, *and Enterprise Connector*.
2. Postępuj zgodnie z krokami wstępnego wdrażania i instalowania aplikacji MobileIron Core opisanymi w rozdziale 1 przewodnika instalowania *On-Premise Installation Guide for MobileIron Core*, *Sentry*, *and Enterprise Connector* dla wersji systemu MobileIron wdrażanej w danym środowisku. W naszym wdrożeniu laboratoryjnym zainstalowaliśmy system MobileIron Core 9.5.0.0 jako wirtualny rdzeń (*ang. Virtual Core*) działający w środowisku VMware 6.0. Po instalacji przeprowadziliśmy aktualizację do wersji 9.7.0.1 systemu MobileIron Core, postępując zgodnie ze wskazówkami zawartymi w dokumencie *CoreConnectorReleaseNotes9701_Rev12Apr2018*. Bezpośrednia instalacja MobileIron Core 9.7.0.1 przyniesie nieco inne rezultaty, ponieważ z niektórych funkcji dodanych w tej wersji nie można korzystać w przypadku wcześniejszych wersji plików konfiguracyjnych.

2.4.2. OGÓLNA KONFIGURACJA SYSTEMU MOBILEIRON CORE

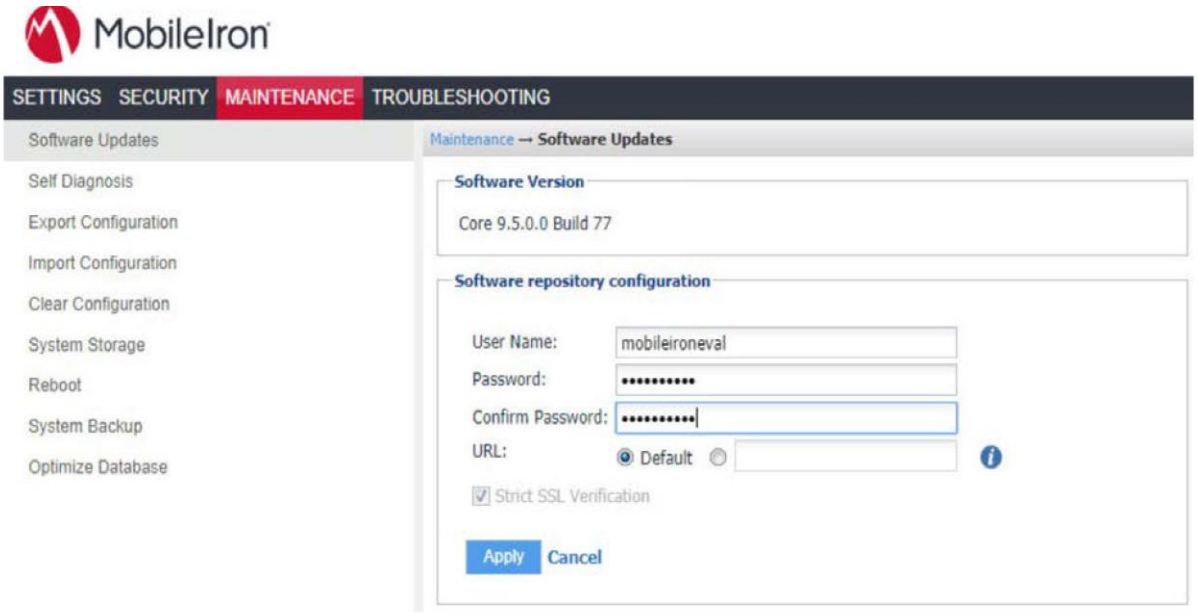
Aby zarejestrować urządzenia mobilne w systemie MobileIron, administratorzy lub użytkownicy powinni wykonać następujące kroki.

1. Pobierać kopię przewodnika po zarządzaniu urządzeniami w systemie *MobileIron Core Device Management Guide for iOS Devices* z portalu pomocy technicznej MobileIron.
2. Wykonać wszystkie instrukcje zawarte w rozdziale 1, „Zadania konfiguracyjne”.

2.4.3. AKTUALIZACJA SYSTEMU MOBILEIRON CORE

Poniższe kroki zostały wykonane w celu uaktualnienia systemu MobileIron Core z wersji 9.5.0.0 do 9.7.0.1. Należy zaznaczyć, że nie było bezpośredniej ścieżki aktualizacji między tymi dwiema wersjami — wybrana przez nas ścieżka aktualizacji to 9.5.0.0 > 9.5.0.1 > 9.7.0.1.

1. Uzyskaj poświadczenia aktualizacji od działu pomocy technicznej MobileIron.
2. W aplikacji **MobileIron Core System Manager** wybierz kolejno **Maintenance** (Konserwacja) > **Software Updates** (Aktualizacje oprogramowania).
3. W obszarze **Software repository Configuration** (konfiguracji repozytorium oprogramowania):
    a. W polu **User Name** (Nazwa użytkownika) wprowadź nazwę użytkownika dostarczoną przez dział pomocy technicznej MobileIron.
    b. W polu **Password** (Hasło) wprowadź hasło dostarczone przez dział pomocy technicznej MobileIron.
    c. W polu **Confirm Password** (Potwierdź hasło) wprowadź ponownie hasło dostarczone przez dział pomocy technicznej MobileIron.
    d. Kliknij przycisk **Apply** (Zastosuj).



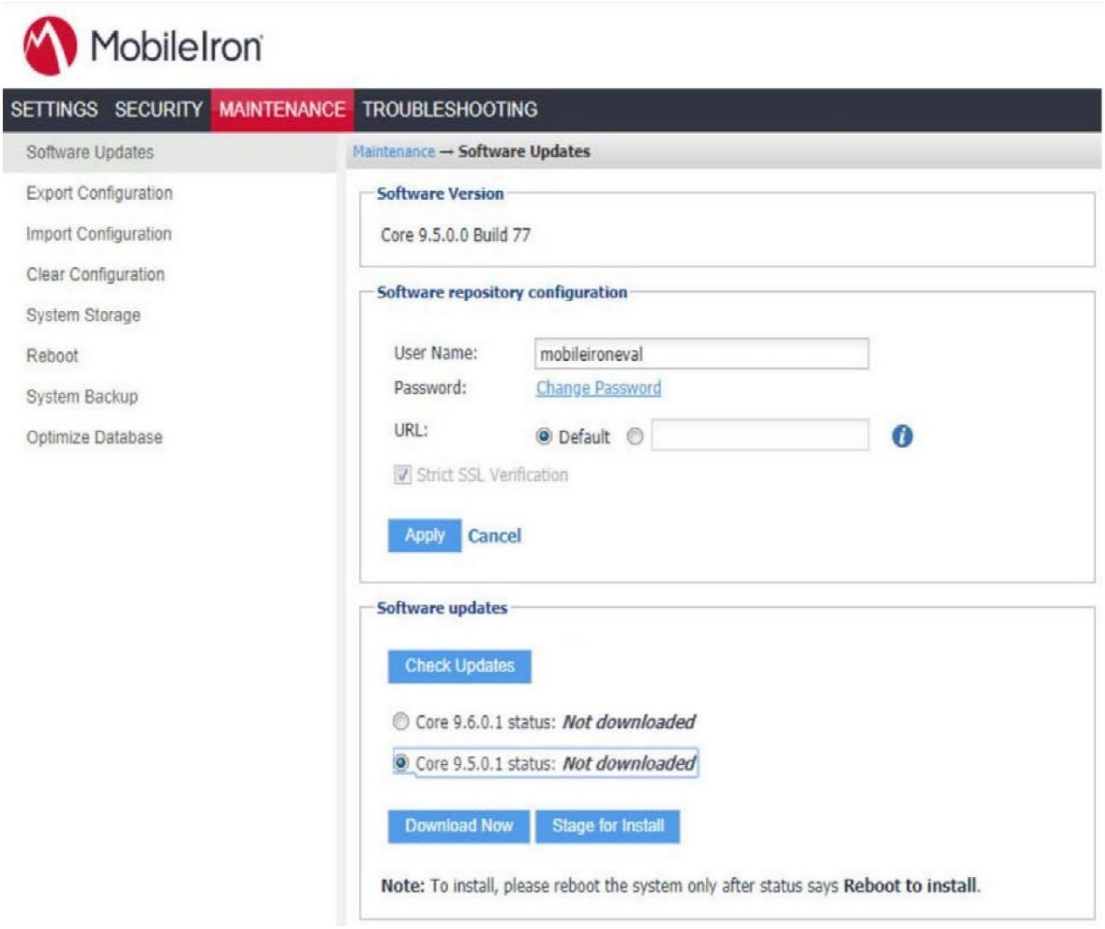
Rysunek 2-1 Konfiguracja repozytorium systemu MobileIron

4. W obszarze **Software Updates** (Aktualizacje oprogramowania):
    a. Kliknij przycisk **Check Updates** (Sprawdź aktualizacje). Po kilku sekundach pojawi się lista dostępnych ścieżek aktualizacji.

Tłumaczenie

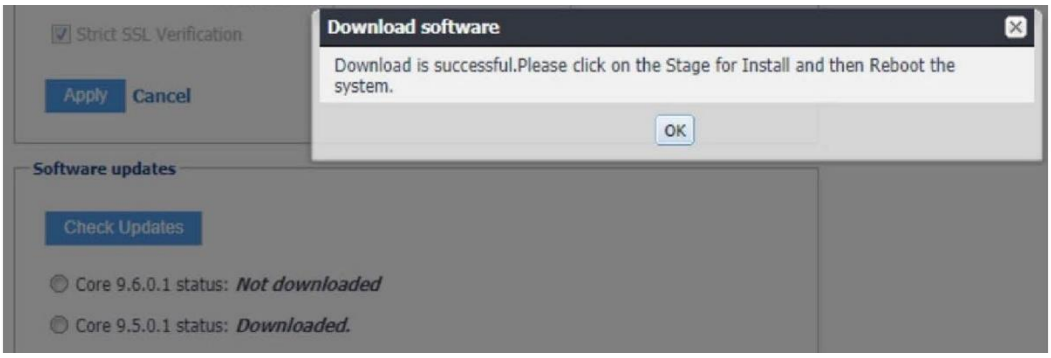
b. Wybierz opcję Core 9.5.0.1 status: **Not Downloaded** (Status Core 9.5.0.1: nie pobrano).

c. Kliknij przycisk **Download Now** (Pobierz teraz). Po chwili pojawi się okno dialogowe **Software Download** (Pobieranie oprogramowania).



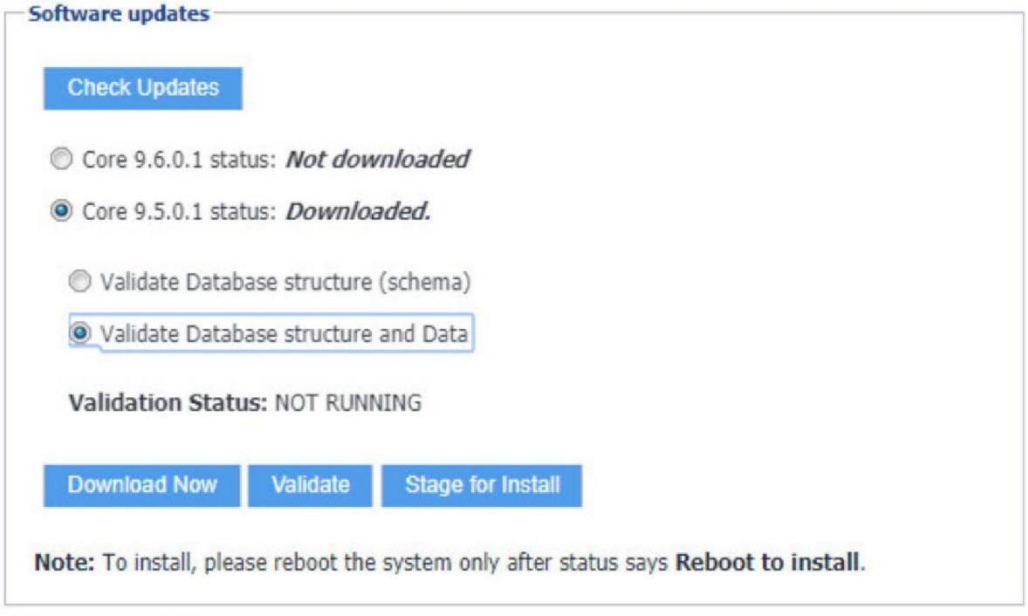
Rysunek 2-2 Wersja systemu MobileIron Core

5. W oknie dialogowym **Download Software** (Pobieranie oprogramowania) kliknij przycisk **OK**.



Rysunek 2-3 Status pobierania systemu MobileIron

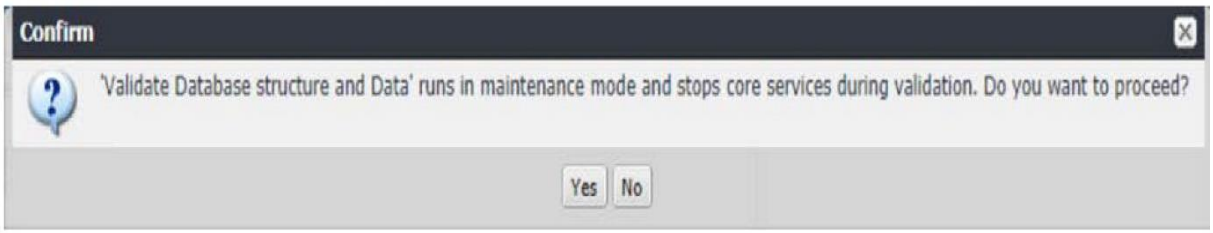
6. W obszarze **Software updates** (Aktualizacje oprogramowania)
   a. Wybierz opcję **Core 9.5.0.1 status: Downloaded** (Status Core 9.5.0.1: pobrano).
   b. Zaznacz opcję **Validate Database Structure and Data** (Sprawdź strukturę i dane bazy danych).
   c. Kliknij przycisk **Validate** (Sprawdź).



Rysunek 2-4 Sprawdzanie poprawności danych w bazie danych

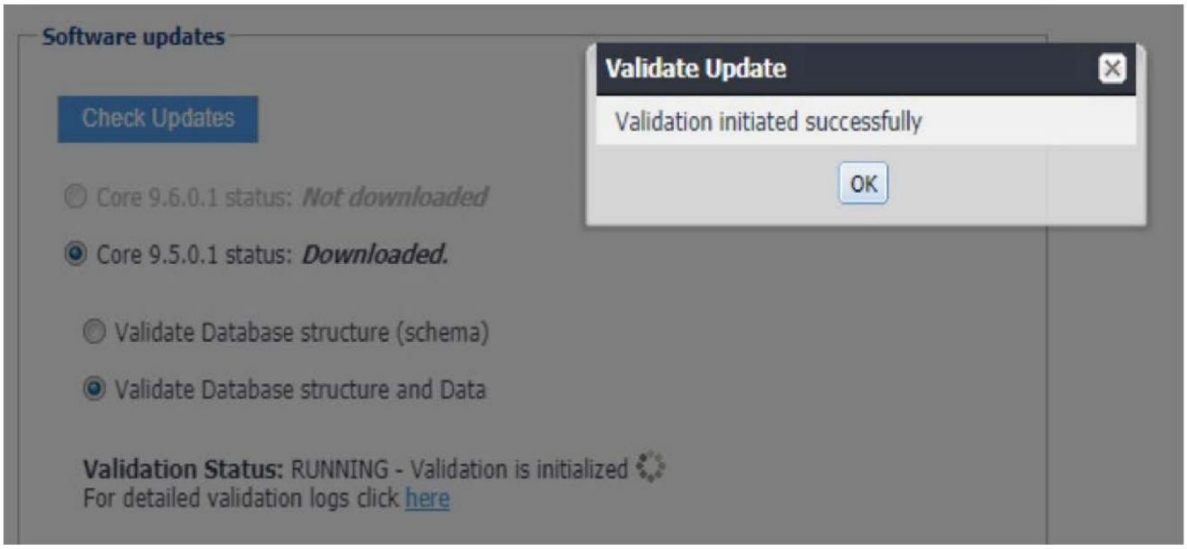
7. W oknie dialogowym **Confirm** (Potwierdź) kliknij przycisk **Yes** (Tak), aby zweryfikować strukturę i dane bazy danych.

Tłumaczenie



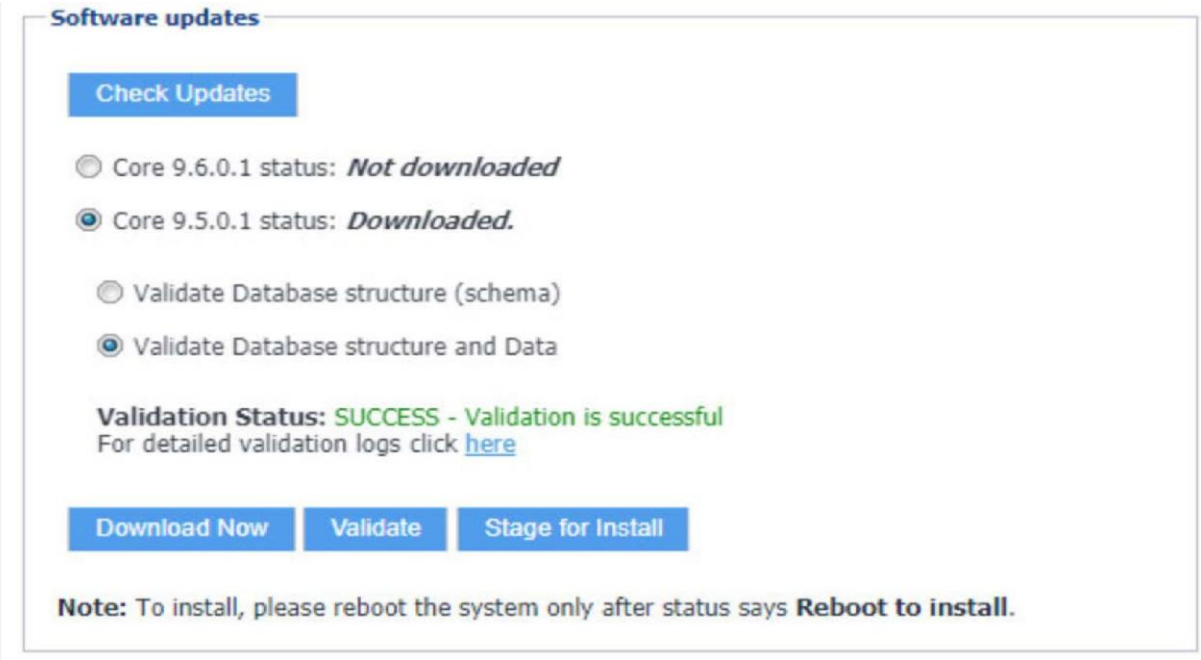
Rysunek 2-5 Potwierdzenie sprawdzenia poprawności danych w bazie danych

8. W oknie dialogowym **Validate Update** (Sprawdzanie poprawności aktualizacji) kliknij przycisk **OK**.



Rysunek 2-6 Potwierdzenie rozpoczęcia sprawdzania poprawności danych w bazie danych

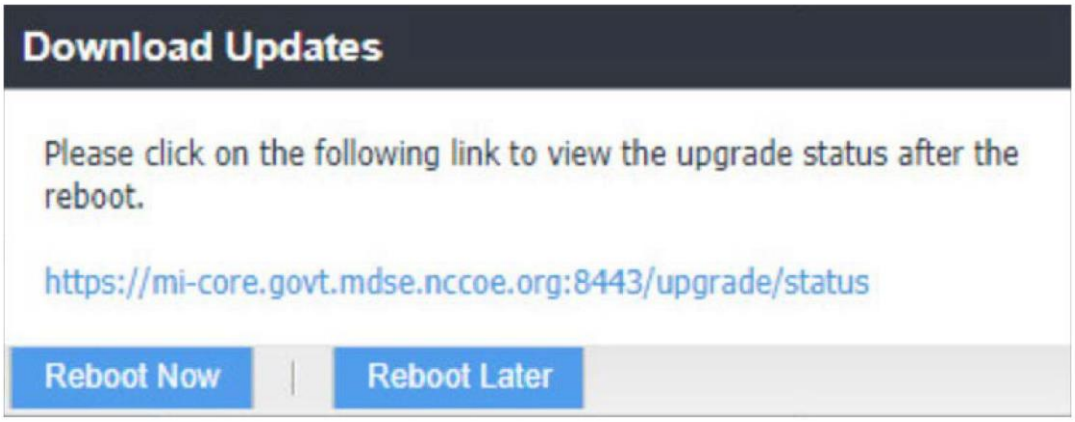
9. W obszarze **Software updates** (Aktualizacje oprogramowania) wybierz opcję **Stage for Install** (Przygotuj do instalacji).



Rysunek 2-7 Status sprawdzania poprawności danych w bazie danych

a. Zostanie wyświetlone okno dialogowe **Download Updates** (Pobierz aktualizacje).

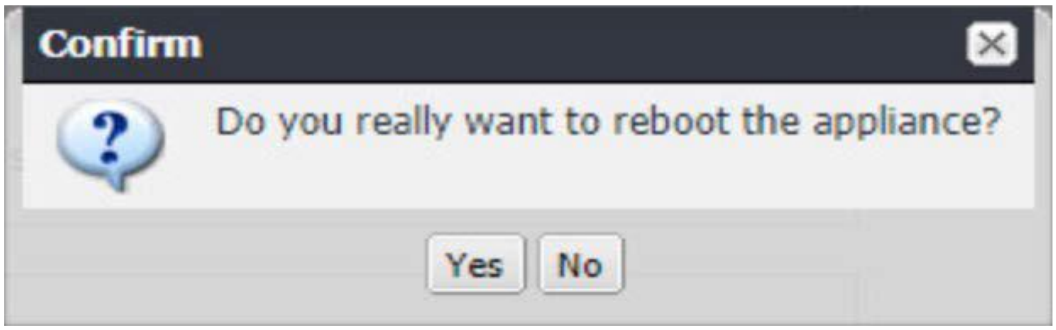
10. W oknie dialogowym **Download Updates** (Pobierz aktualizacje) kliknij przycisk **Reboot Now** (Uruchom ponownie teraz). Pojawi się seria okien dialogowych.



Rysunek 2-8 Informacja o konieczności ponownego uruchomienia w celu aktualizacji oprogramowania

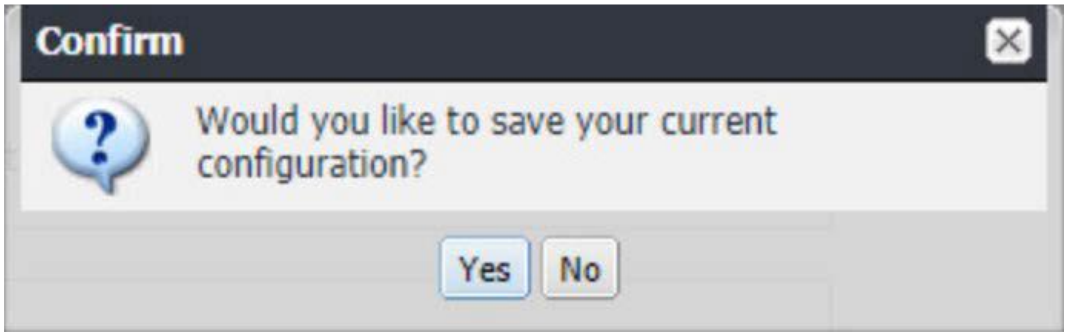
11. W oknach dialogowych **Confirm** (Potwierdź):

a. Kliknij przycisk **Yes** (Tak), aby potwierdzić ponowne uruchomienie urządzenia.



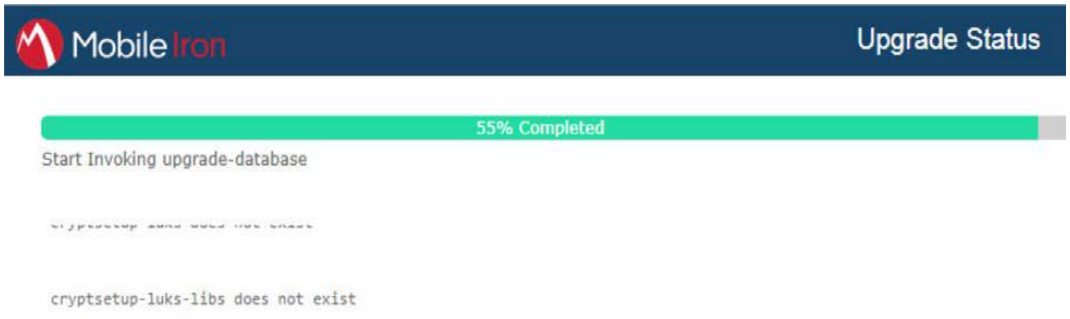
Rysunek 2-9 Potwierdzenie ponownego uruchomienia w celu aktualizacji oprogramowania

b. Kliknij przycisk **Yes** (Tak), aby potwierdzić zapisanie bieżącej konfiguracji.



Rysunek 2-10 Informacja o możliwości zapisania konfiguracji przed ponownym uruchomieniem

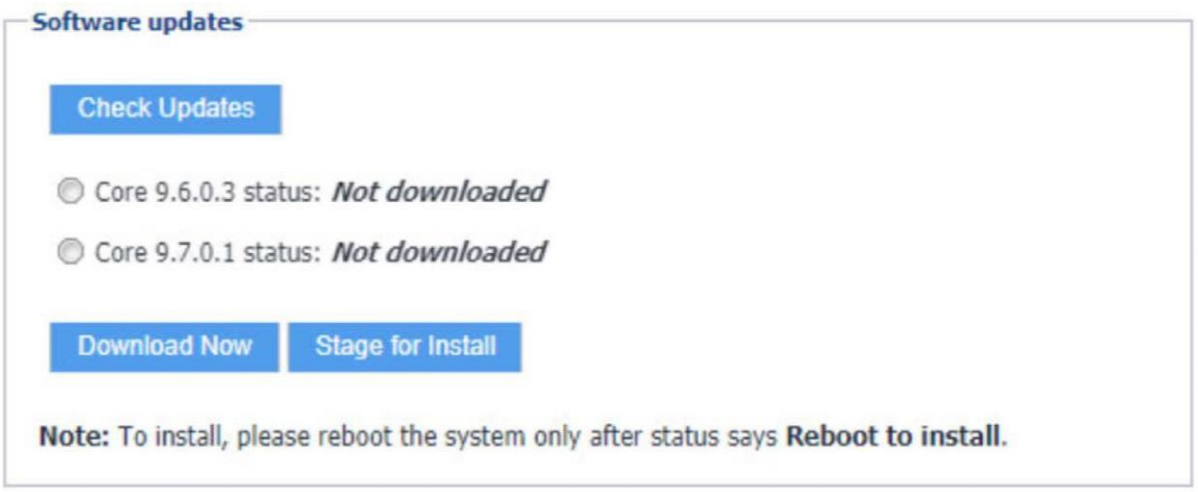
12. Witryna Upgrade Status (Stan aktualizacji) hostowana przez Core zostanie automatycznie otwarta.



Rysunek 2-11 Stan aktualizacji

13. Po zakończeniu aktualizacji w części **System Manager** (Menedżer systemu) > **Maintenance** (Konserwacja) > **Software Updates** (Aktualizacje oprogramowania) wyświetlana jest możliwość aktualizacji do wersji 9.7.0.1.

Tłumaczenie



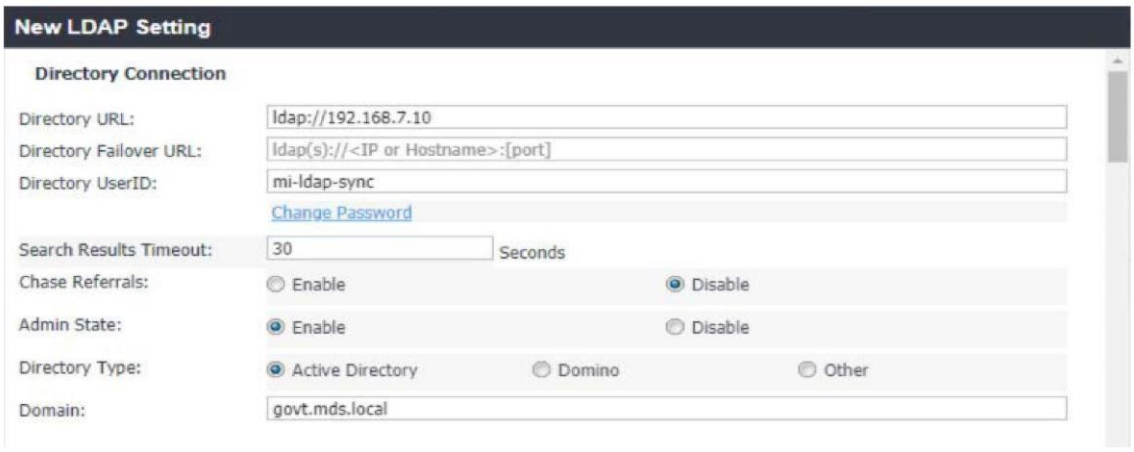
Rysunek 2-12 Możliwość aktualizacji do wersji 9.7.0.1

14. Powtórz kroki od 4b do 11 powyżej, zastępując wersję 9.5.0.1 wersją 9.7.0.1 w krokach 4b i 6. Zakończy to ścieżkę aktualizacji systemu MobileIron Core z wersji 9.5.0.0 do wersji 9.7.0.1.

2.4.4. INTEGRACJA Z USŁUGĄ MICROSOFT ACTIVE DIRECTORY

W naszym wdrożeniu zdecydowaliśmy się na integrację systemu MobileIron Core z usługą Active Directory przy użyciu protokołu Lightweight Directory Access Protocol (LDAP). Ten krok jest opcjonalny. Ogólne instrukcje dotyczące tego procesu znajdują się w punkcie *Configuring LDAP Servers* w rozdziale 2 podręcznika *On-Premise Installation Guide for MobileIron Core, Sentry and Enterprise Connector*. Szczegółowe informacje dotyczące konfiguracji wykorzystane podczas wykonywania wybranych kroków (z zachowaniem oryginalnej numeracji) z tego przewodnika podano poniżej:

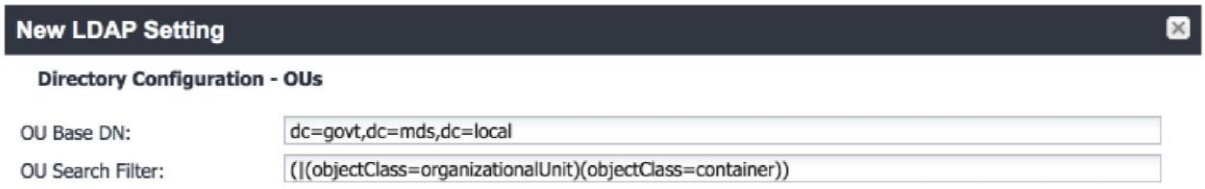
1. Z kroku 4 w przewodniku MobileIron, w oknie dialogowym **New LDAP Server** (Nowy serwer LDAP):
   a. Directory Connection (Połączenie z katalogiem):



Rysunek 2-13 Ustawienia protokołu LDAP

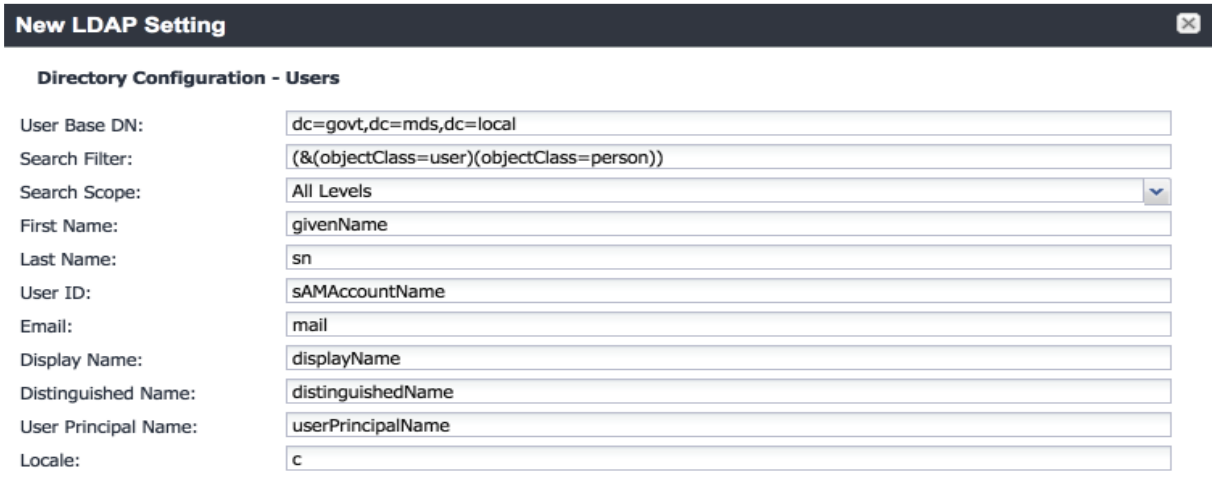
Uwaga: Jasnoszary tekst jest tekstem domyślnym. Należy wprowadzić własny adres URL katalogu.

b. Directory Configuration (Konfiguracja katalogu) – OUs (Jednostki organizacyjne):



Rysunek 2-14 Jednostki organizacyjne protokołu LDAP

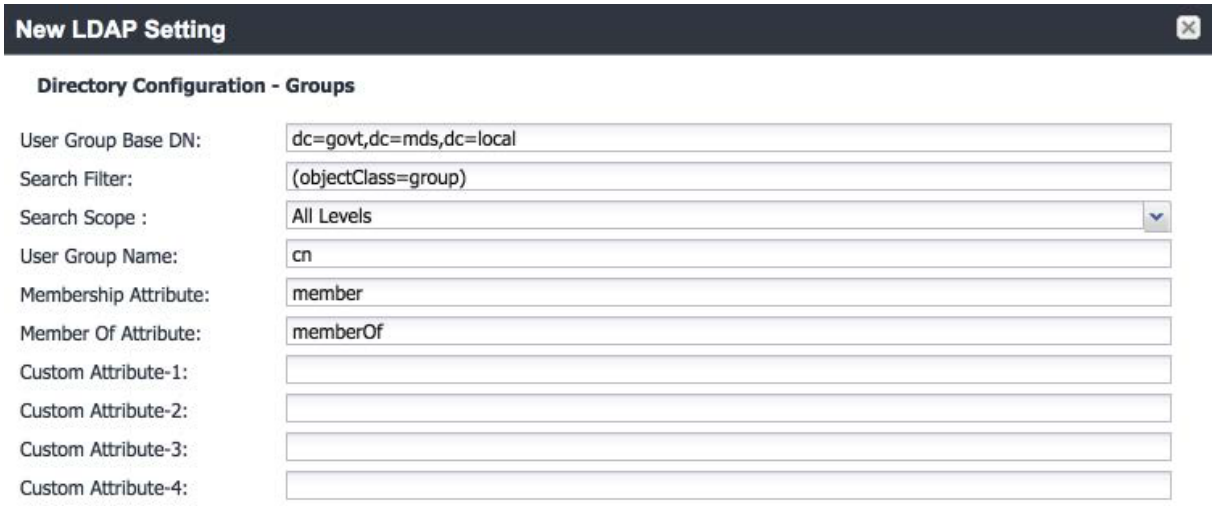
c. Directory Configuration (Konfiguracja katalogu) – Users (Użytkownicy):



Rysunek 2-15 Konfiguracja użytkownika protokołu LDAP

Tłumaczenie

d. Directory Configuration (Konfiguracja katalogu) – Groups (Grupy)



Rysunek 2-16 Konfiguracja grupy protokołu LDAP

e. Grupy LDAP:

i. Na początek wykorzystaliśmy użytkowników i komputery zarejestrowane w usłudze Active Directory do utworzenia nowej grupy zabezpieczeń dla autoryzowanych użytkowników mobilnych na kontrolerze domeny dla domeny govt.mds.local. W naszym przykładzie grupa ta nosi nazwę **Mobile Users** (Użytkownicy mobilni).

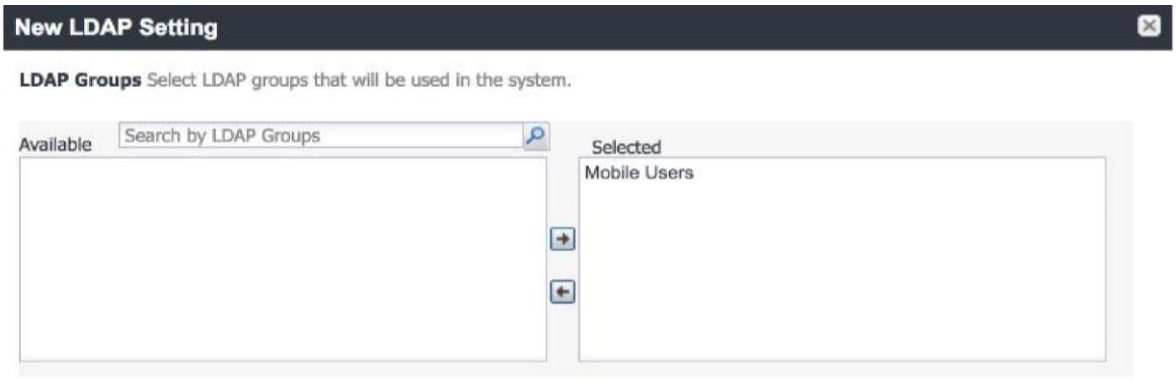
ii. W pasku wyszukiwania wprowadź nazwę grupy LDAP dla użytkowników z autoryzacją mobilną.

iii. Kliknij **przycisk lupy**. Nazwa grupy powinna zostać dodana do listy **Available** (Dostępne).

iv. W polu listy **Available** (Dostępne):

1) Wybierz pozycję z listy o nazwie **Mobile Users** (Użytkownicy mobilni).

2) Kliknij przycisk **strzałki w prawo**. Pozycja z listy o nazwie **Mobile Users** (Użytkownicy mobilni) powinna zostać przeniesiona do pola **Selected** (Wybrane).



Rysunek 2-17 Wybrana grupa LDAP

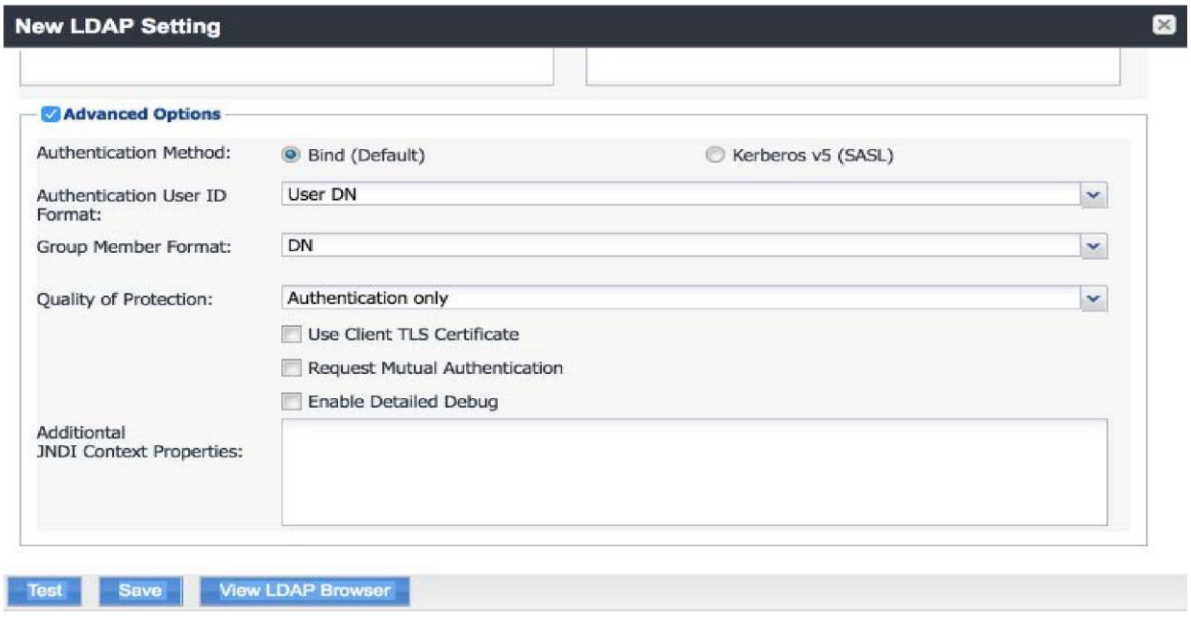
v. Na liście **Selected** (Wybrane):

1) Wybierz domyślną pozycję listy grup **Users** (Użytkownicy).

2) Kliknij przycisk **strzałki w lewo**. Pozycja z listy o nazwie **Users** (Użytkownicy) powinna zostać przeniesiona do listy **Available** (Dostępne).

f. Ustawienia niestandardowe: Ustawienia niestandardowe nie zostały określone.

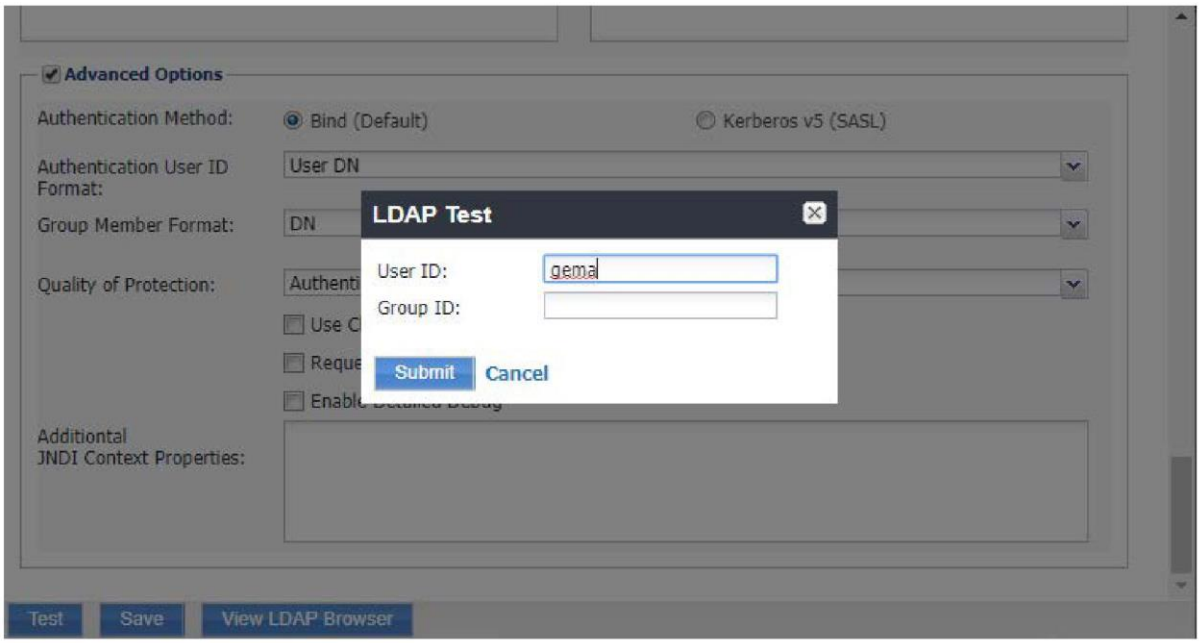
g. Opcje zaawansowane: Opcje zaawansowane zostały skonfigurowane w sposób zaprezentowany na rysunku 2-18.



Rysunek 2-18 Zaawansowane opcje LDAP

Uwaga: W naszym środowisku laboratoryjnym nie skorzystaliśmy z opcji silniejszej jakości ochrony (*ang. Quality of Protection*), korzystania z certyfikatu TLS lub żądania wzajemnego uwierzytelniania. Zalecamy jednak, aby osoby odpowiedzialne za wdrożenie rozważyły użycie tych dodatkowych mechanizmów w celu zabezpieczenia komunikacji z serwerem LDAP.

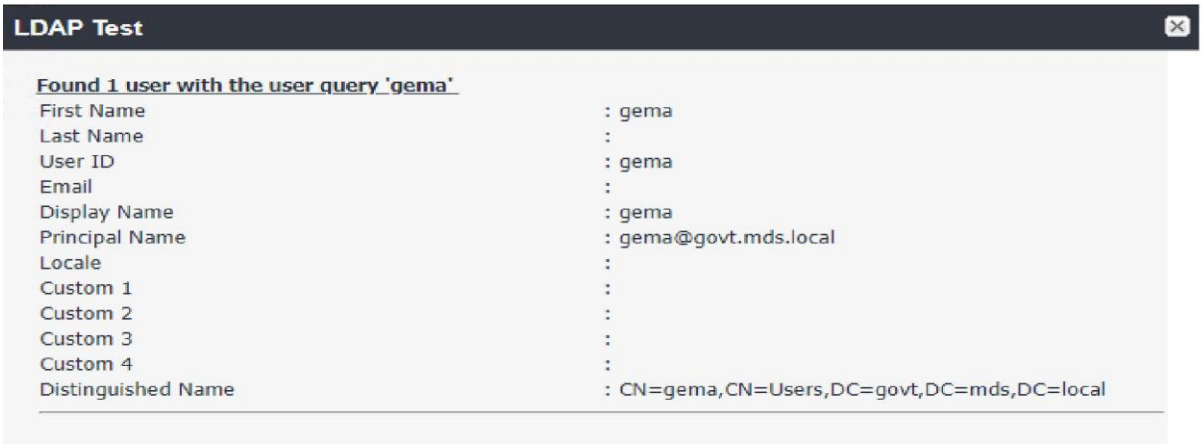
2. W krokach od 19 do 21 z przewodnika MobileIron sprawdziliśmy, czy system MobileIron może pomyślnie wysyłać zapytania do serwera LDAP w celu uzyskania pochodnych danych uwierzytelniających tożsamość osobistą (*ang. Derived PIV Credential – DPC*) użytkowników.
    a. W oknie dialogowym **New LDAP Setting** (Ustawianie nowego serwera LDAP) kliknij przycisk **Test** (Testuj), aby otworzyć okno dialogowe **LDAP Test** (Test LDAP).
    b. W oknie dialogowym **LDAP Test** (Test LDAP) wypełnij pole **User ID** (Identyfikator użytkownika) dla danego użytkownika DPC, a następnie kliknij przycisk **Submit** (Prześlij). Członkiem grupy **Mobile Users** (Użytkownicy mobilni) w naszym środowisku jest **gema**.



Rysunek 2-19 Testowanie konfiguracji serwera LDAP

Tłumaczenie

c. Okno dialogowe **LDAP Test** (Test LDAP) wskazuje, że zapytanie powiodło się

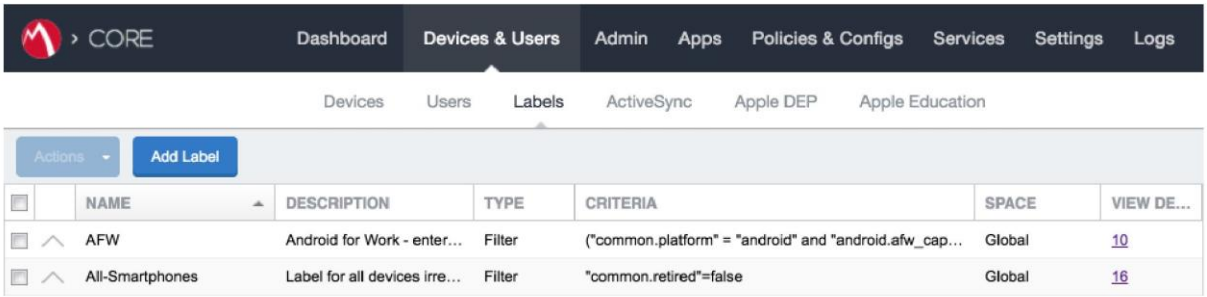


Rysunek 2-20 Wynik testu serwera LDAP

2.4.5. TWORZENIE ETYKIET UŻYTKOWNIKÓW MOBILNYCH

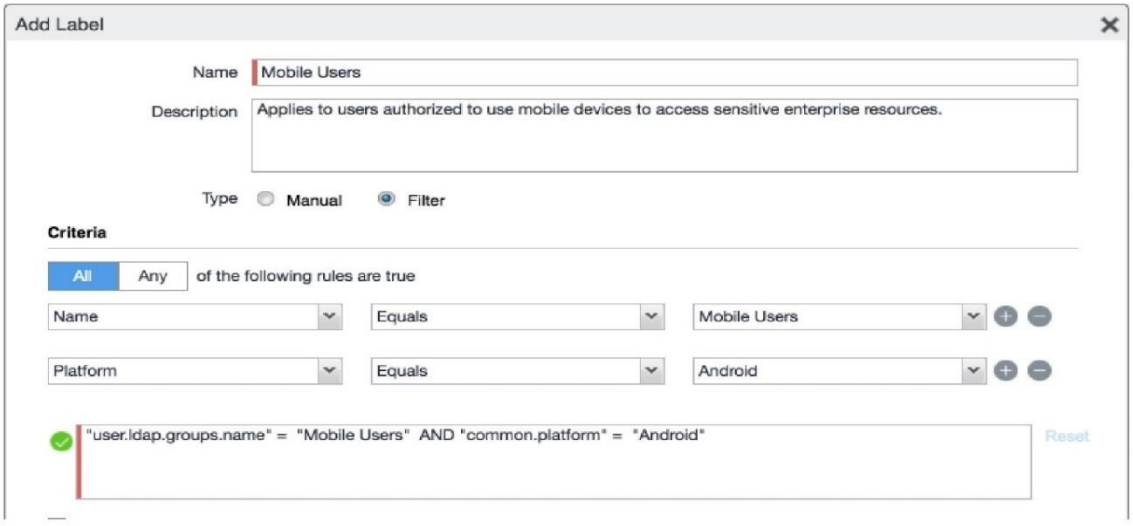
W systemie MobileIron stosuje się etykiety w celu powiązania zasad i konfiguracji urządzeń z użytkownikami i urządzeniami mobilnymi. Utworzenie unikalnej etykiety dla każdej kategorii autoryzowanych użytkowników mobilnych umożliwia administratorom tych urządzeń zastosowanie spójnego zestawu środków bezpieczeństwa dla użytkowników korzystających z urządzeń mobilnych w podobny sposób. Nasz ograniczony scenariusz użytkowania wymagał utworzenia tylko jednej etykiety w systemie MobileIron.

1. Na stronie **MobileIron Core Admin Portal** przejdź do części **Devices & Users** (Urządzenia i użytkownicy) > **Labels** (Etykiety).
2. Kliknij przycisk **Add Label** (Dodaj etykietę).



Rysunek 2-21 Etykiety urządzeń w systemie MobileIron

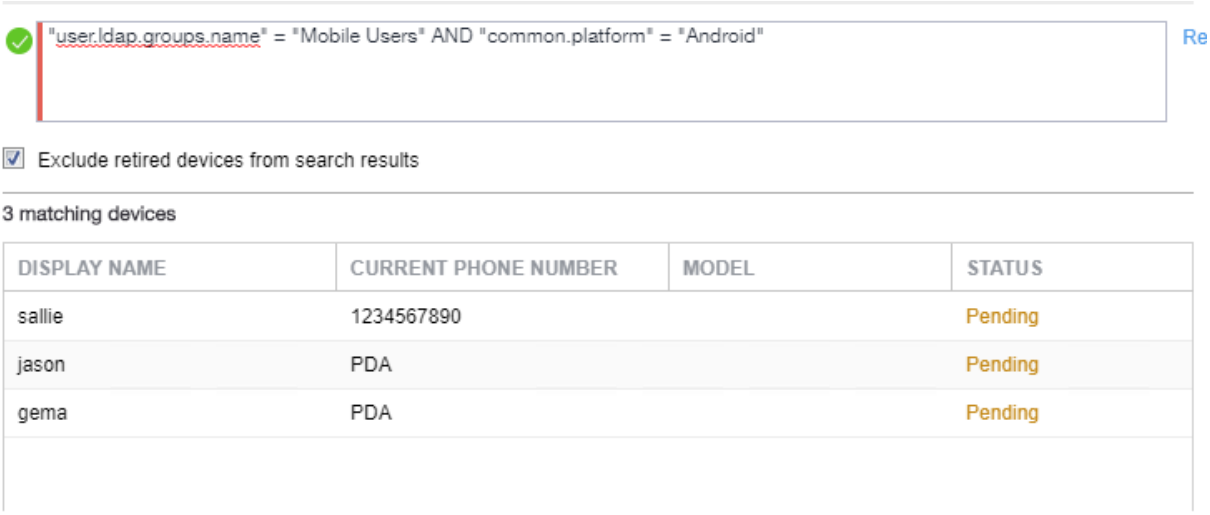
3. W polu **Name** (Nazwa) wprowadź unikalną nazwę dla tej etykiety (w tym przykładzie **Mobile Users**).
4. W polu **Description** (Opis) wprowadź merytoryczny opis, który umożliwi innym zidentyfikowanie celu jej utworzenia.
5. W części **Criteria** (Kryteria):
    a. W pustej regule:
        i. Z menu rozwijanego **Field** (Pole) wybierz kolejno opcje **User** (Użytkownik) > **LDAP** > **Groups** (Grupy) > **Name** (Nazwa).
        ii. Z menu rozwijanego **Value** (Wartość) wybierz grupę Active Directory utworzoną w celu obsługi zasad użytkowników mobilnych (w tym przykładzie nazwaną **Mobile User**).
    b. Kliknij **ikonę ze znakiem plus**, aby dodać pustą regułę.
    c. W nowo utworzonej pustej regule:
        i. W menu rozwijanym **Field** (Pole) wybierz **Common** (Wspólne) > **Platform** (Platforma).
        ii. Z menu rozwijanego **Value** (Wartość) wybierz opcję **Android**.



Rysunek 2-22 Dodawanie etykiety urządzenia

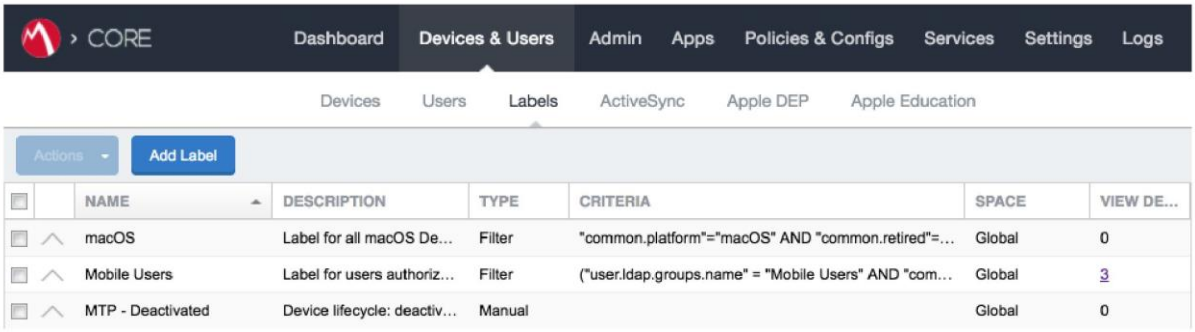
d. Lista pasujących urządzeń zostanie wyświetlona pod podanymi kryteriami.

e. Kliknij przycisk **Save** (Zapisz).



Rysunek 2-23 Dopasowania do etykiety urządzenia

6. Przejdź do części **Devices & Users** (Urządzenia i użytkownicy) > **Labels** (Etykiety), aby się upewnić, że etykieta została pomyślnie utworzona.



Rysunek 2-24 Lista etykiet w systemie MobileIron

2.5. INTEGRACJA APLIKACJI PALO ALTO NETWORKS GLOBALPROTECT Z SYSTEMEM MOBILEIRON

W poniższych krokach szczegółowo opisano, jak zintegrować system MobileIron Core, usługę Microsoft Certificate Authority (CA) i aplikację Palo Alto Networks GlobalProtect, aby umożliwić użytkownikom mobilnym uwierzytelnianie się w bramie

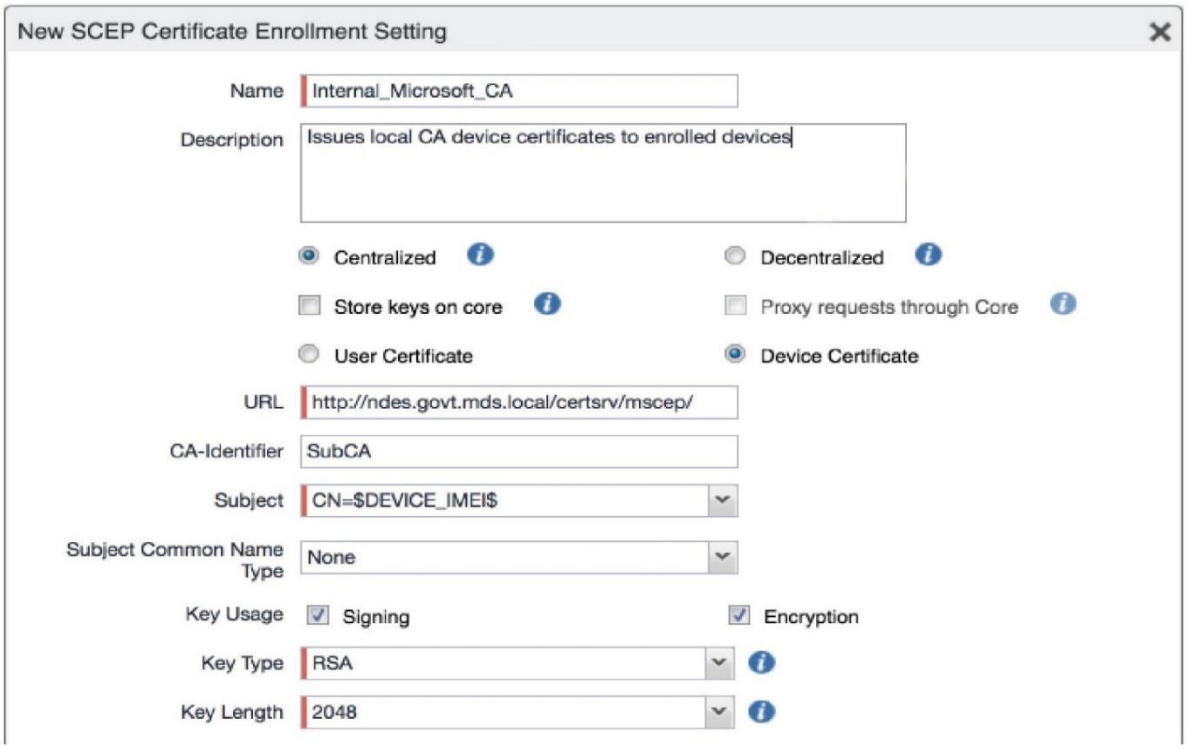
GlobalProtect przy użyciu certyfikatów urządzeń z rozpoznawaniem użytkowników przypisanych do urządzeń mobilnych przez usługę Microsoft CA podczas rejestracji w systemie MobileIron Core.

2.5.1. KONFIGURACJA SYSTEMU MOBILEIRON

Poniższe kroki umożliwiają utworzenie konfiguracji systemu MobileIron Core niezbędnej do integracji z aplikacją Palo Alto Networks GlobalProtect i usługą Microsoft CA.

2.5.1.1. KONFIGUROWANIE PROTOKOŁU SCEP (ANG. SIMPLE CERTIFICATE ENROLMENT PROTOCOL)

1. Na stronie **MobileIron Core Admin Portal** przejdź do obszaru **Policies & Configs** (Zasady i konfiguracja) > **Configurations** (Konfiguracje).
2. Wybierz kolejno opcje **Add New** (Dodaj nową) > **Certificate Enrollment** (Rejestracja certyfikatu) > **SCEP**. Zostanie otwarte okno dialogowe **New SCEP Configuration Enrollment Setting** (Ustawianie nowej konfiguracji rejestrowania SCEP).
3. W oknie **New SCEP Configuration Enrollment Setting** (Ustawianie nowej konfiguracji rejestrowania SCEP):
    a. W polu **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi zidentyfikowanie tej konfiguracji.
    b. Włącz opcję **Device Certificate** (Certyfikat urządzenia).
    c. W polu **URL** wprowadź adres URL, pod którym w danym środowisku jest hostowany protokół SCEP.
    d. W polu **CA-Identifier (ID)** (Identyfikator ośrodka certyfikacji) wprowadź nazwę ośrodka certyfikacji Microsoft, który będzie wystawiał certyfikaty urządzeń.
    e. Z rozwijanego menu **Subject** (Podmiot) wybierz pozycję **$DEVICE_IMEI$**.



Rysunek 2-25 Konfiguracja protokołu SCEP w systemie MobileIron

f. W polu **Fingerprint** (Cyfrowy odcisk palca) wprowadź odcisk palca ośrodka certyfikacji Microsoft, który będzie wystawiać certyfikaty dla urządzeń.

g. Z menu rozwijanego **Challenge Type** (Typ połączenia) wybierz opcję **Microsoft SCEP**.

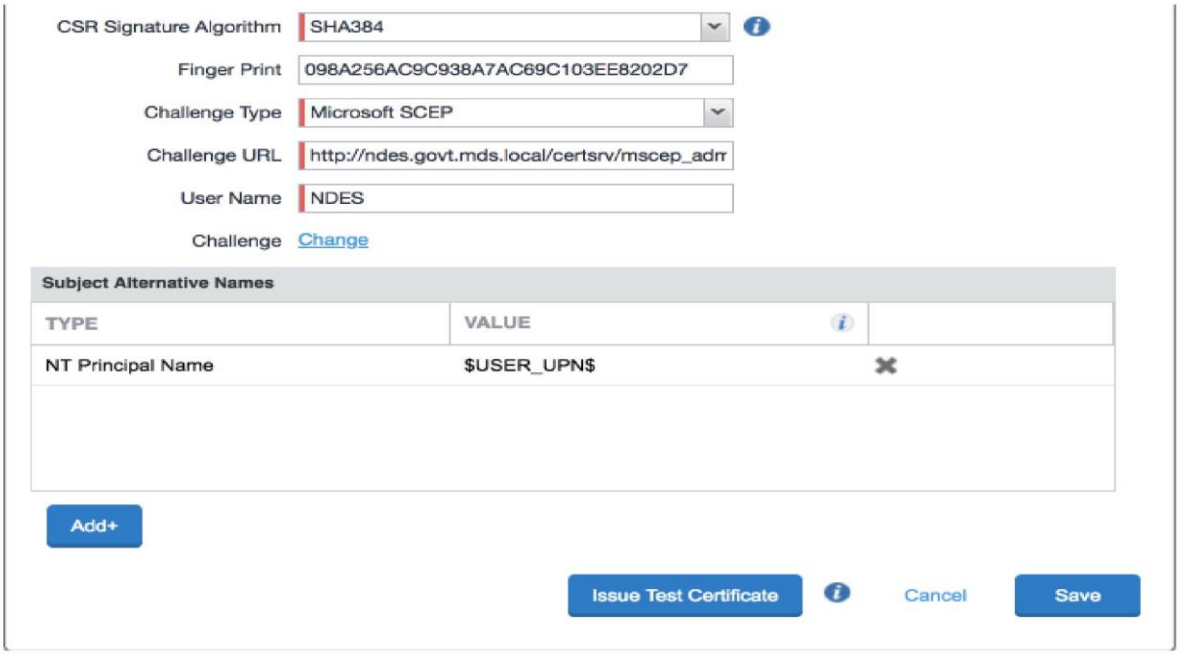
h. Kliknij przycisk **Add** (Dodaj) znajdujący się pod polem listy **Subject Alternative Names** (Alternatywne nazwy podmiotów). Na liście pojawi się nowa pozycja.

i. Dla nowej pozycji na liście:

   i. Z menu rozwijanego **Type** (Typ) wybierz opcję **NT Principal Name** (Główna nazwa NT).

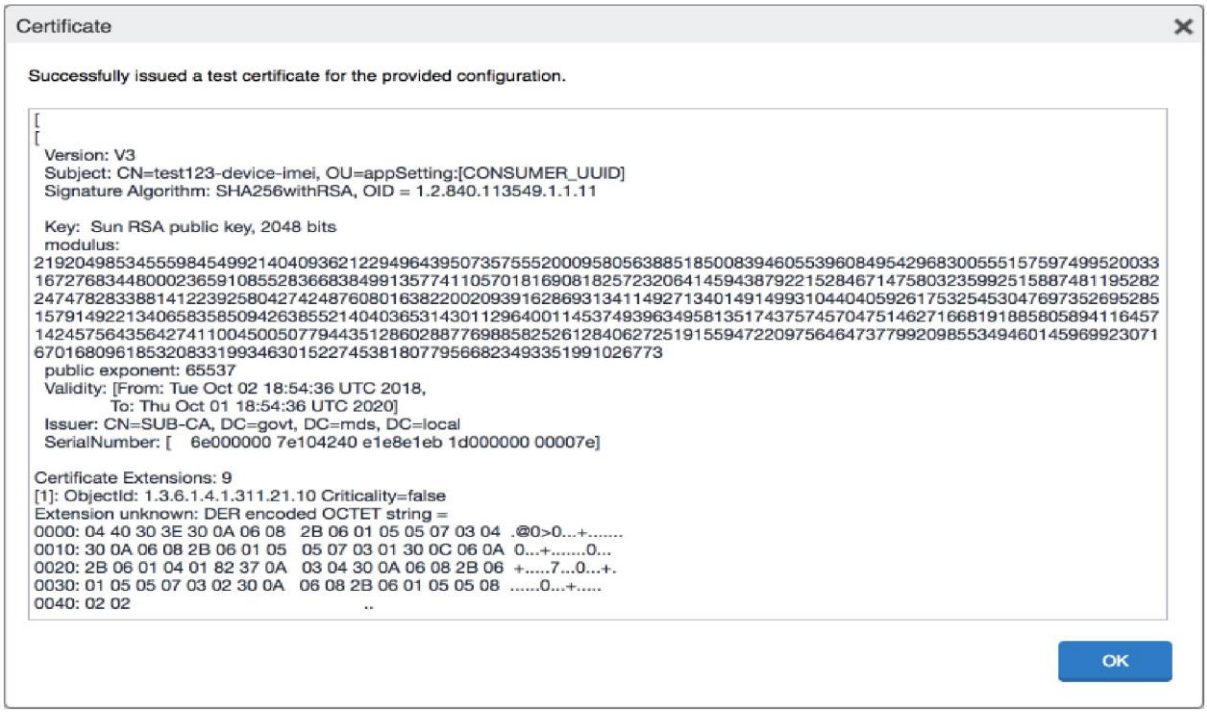
   ii. Z menu rozwijanego **Value** (Wartość) wybierz opcję **$USER_UPN$**.

j. Kliknij przycisk **Issue Test Certificate** (Wystaw certyfikat testowy). W oknie dialogowym **Certificate** (Certyfikat) powinien pojawić się komunikat o powodzeniu.



Rysunek 2-26 Test konfiguracji certyfikatu SCEP

k. W oknie dialogowym **Certificate** (Certyfikat) kliknij przycisk **OK**.



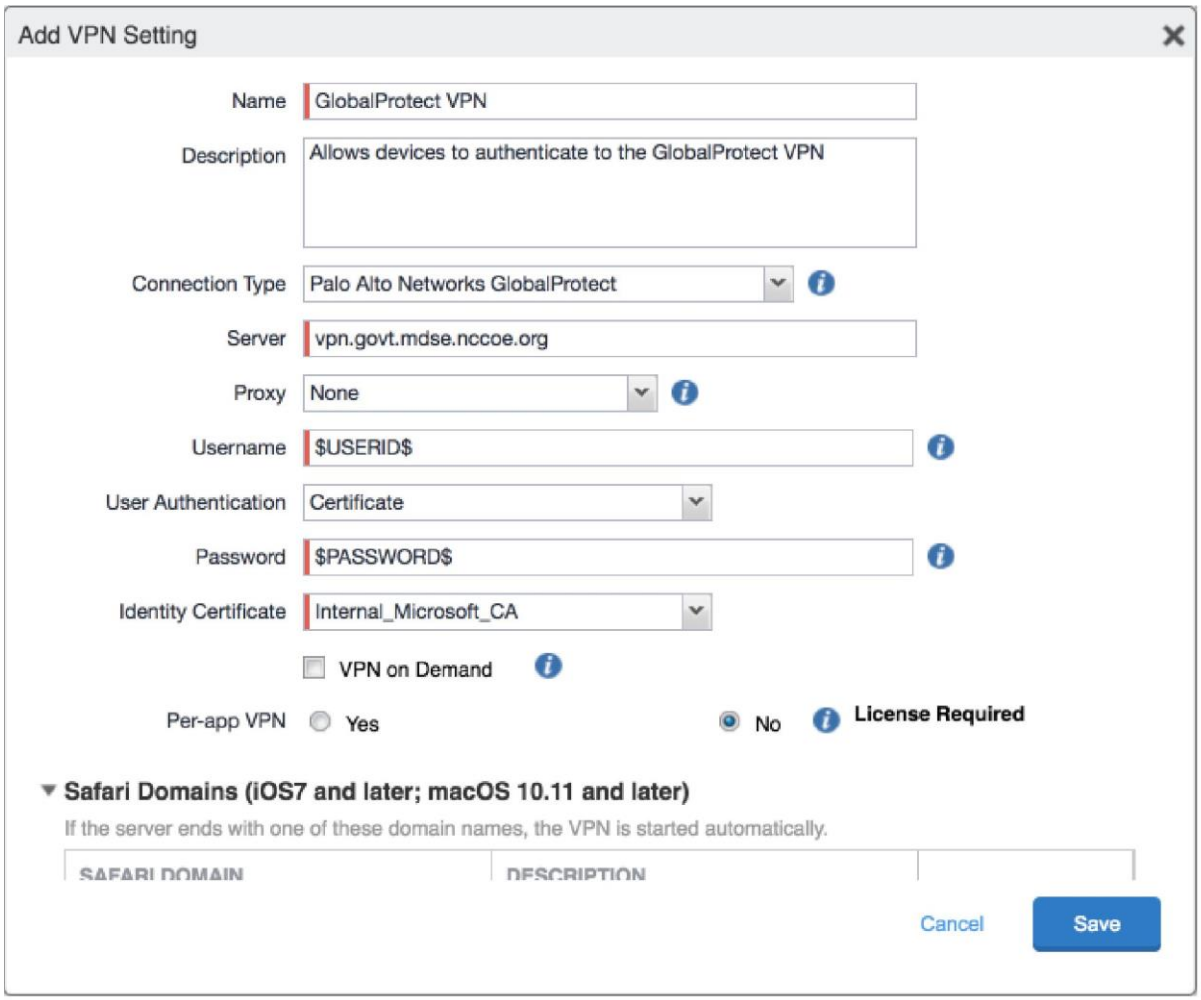
Rysunek 2-27 Test certyfikatu SCEP

4. Kliknij przycisk **Save** (Zapisz).

2.5.1.2. TWORZENIE KONFIGURACJI APLIKACJI PALO ALTO NETWORKS GLOBALPROTECT

Konfiguracja aplikacji GlobalProtect nakazuje klientowi mobilnemu korzystanie z nadanego certyfikatu urządzenia i automatyczne łączenie się z prawidłowym adresem URL sieci VPN. Użytkownicy mobilni nie muszą ręcznie konfigurować aplikacji. W poniższych krokach zostanie utworzona konfiguracja dla aplikacji GlobalProtect.

1. Na stronie **MobileIron Admin Portal** przejdź do **Policies & Configs** (Zasady i konfiguracje) > **Configurations** (Konfiguracje).
2. Wybierz kolejno opcje **Add New** (Dodaj nowe) > **VPN**. Zostanie wyświetlone okno dialogowe **Add VPN Setting** (Dodaj ustawienia sieci VPN).
3. W oknie dialogowym **Add VPN Setting** (Dodaj ustawienia sieci VPN):
    a. W polu **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi identyfikację tych ustawień sieci VPN.
    b. Z menu rozwijanego **Connection Type** (Typ połączenia) wybierz opcję **Palo Alto Networks GlobalProtect**.
    c. W polu **Server** (Serwer) wprowadź w pełni kwalifikowaną nazwę domeny (*ang. Fully Qualified Domain Name – FQDN*) urządzenia Palo Alto Networks. W naszej przykładowej implementacji użyto nazwy **vpn.govt.mdse.nccoe.org**.
    d. Z menu rozwijanego **User Authentication** (Uwierzytelnianie użytkownika) wybierz opcję **Certificate** (Certyfikat).
    e. Z menu rozwijanego **Identity Certificate** (Certyfikat tożsamości) wybierz profil rejestracji SCEP utworzony w poprzednim punkcie.
    f. Kliknij przycisk **Save** (Zapisz).



Rysunek 2-28 Konfiguracja sieci VPN w systemie MobileIron

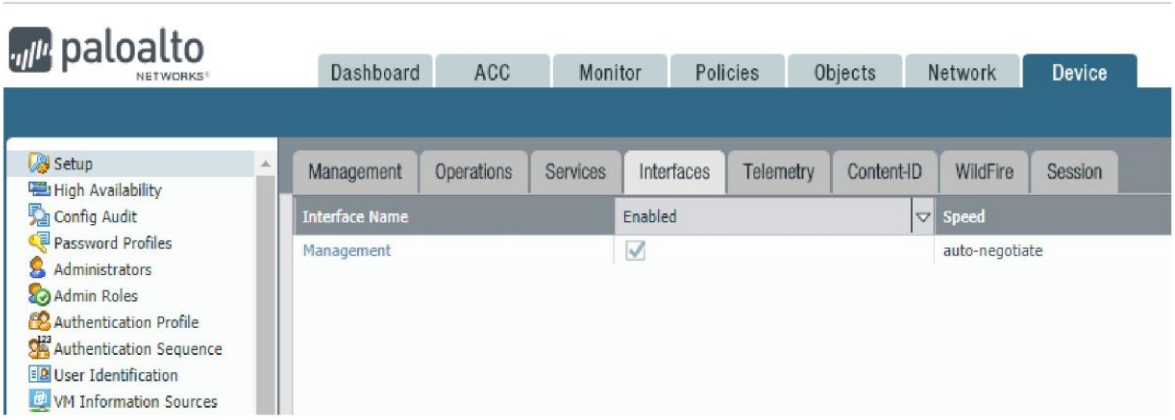
2.5.2. PODSTAWOWA KONFIGURACJA URZĄDZENIA PALO ALTO NETWORKS

Podczas tworzenia podstawowej konfiguracji adresy IP są przypisywane do interfejsu zarządzania, systemu nazw domen (*ang. Domain Name System – DNS*) i sieciowego protokołu synchronizacji czasu (*ang. Network Time Protocol – NTP*). Interfejs zarządzania umożliwia administratorowi konfigurowanie i wdrażanie reguł bezpieczeństwa.

2.5.2.1. KONFIGURACJA INTERFEJSU ZARZĄDZANIA

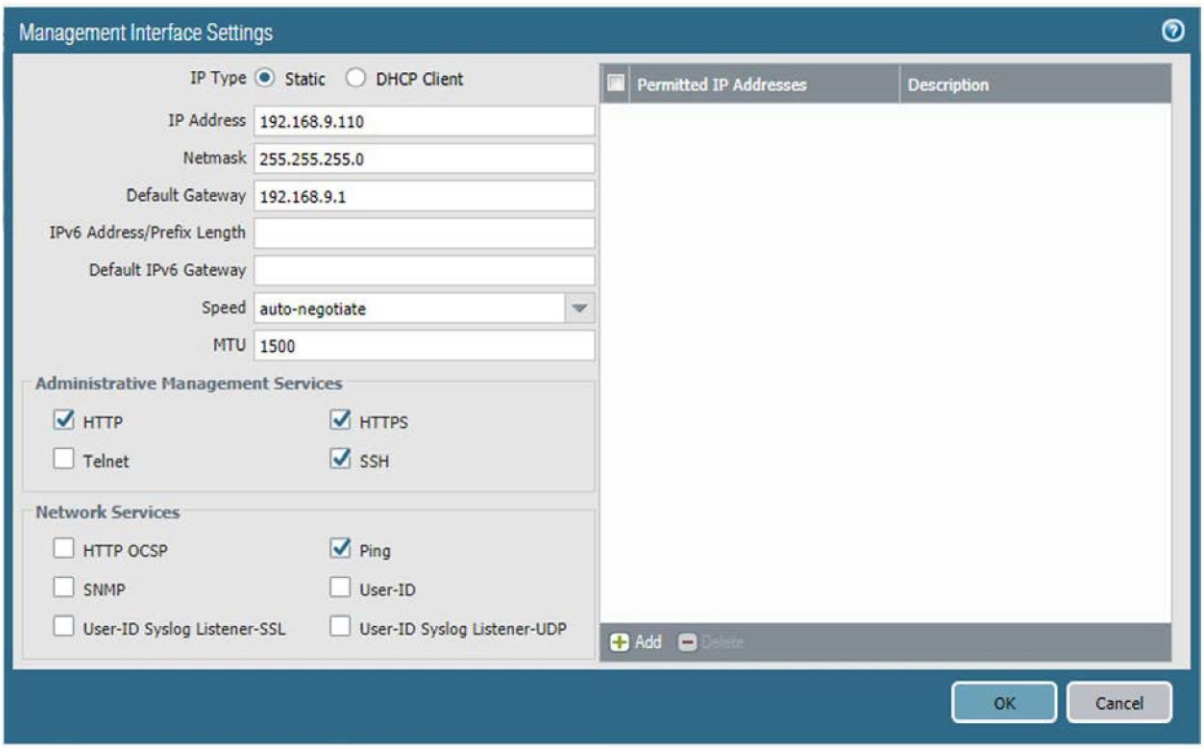
Poniższe kroki umożliwią skonfigurowanie interfejsu zarządzania urządzenia Palo Alto Networks.

1. W portalu Palo Alto Networks wybierz kolejno opcje **Device** (Urządzenie) > **Setup** (Konfiguracja) > **Interfaces** (Interfejsy).
2. Na karcie **Interfaces** (Interfejsy) włącz opcję **Management** (Zarządzanie). Zostanie otwarta strona **Management Interface Setting** (Ustawienia interfejsu zarządzania).



Rysunek 2-29 Włączony interfejs zarządzania Palo Alto Networks

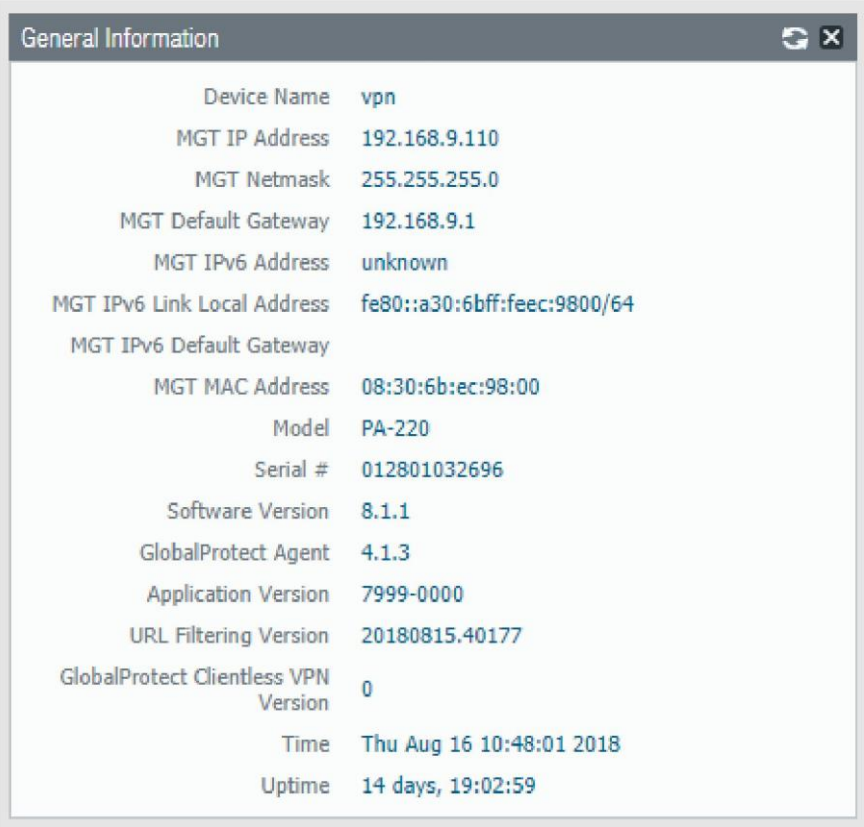
3. Na ekranie **Management Interface Setting** (Ustawienia interfejsu zarządzania):
   a. W polu **IP Address** (Adres IP) wprowadź adres IP urządzenia Palo Alto Networks.
   b. W polu **Netmask** (Maska sieci) wprowadź maskę sieci.
   c. W polu **Default Gateway** (Brama domyślna) wprowadź adres IP routera, który zapewnia urządzeniu dostęp do Internetu.
   d. W obszarze **Administrative Management Services** (Usługi zarządzania administracyjnego): Zaznacz opcje **Hypertext Transfer Protocol (HTTP)**, **Hypertext Transfer Protocol Secure (HTTPS)**, **Secure Shell (SSH)** i **Ping**.
   e. Kliknij przycisk **OK**.



Rysunek 2-30 Konfiguracja interfejsu zarządzania

4. Aby zweryfikować konfigurację, przejdź do **Palo Alto Networks Portal** > **Dashboard** (Pulpit nawigacyjny). W części **General Information** (Informacje ogólne) powinna się znajdować konfiguracja sieciowa urządzenia.

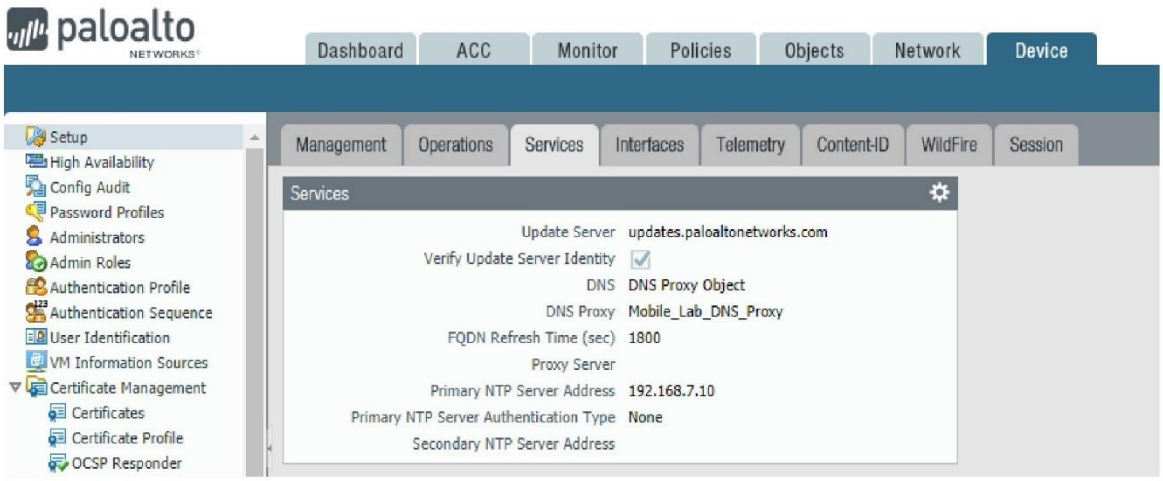
Tłumaczenie



Rysunek 2-31 Informacje ogólne o zaporze sieciowej Palo Alto Networks

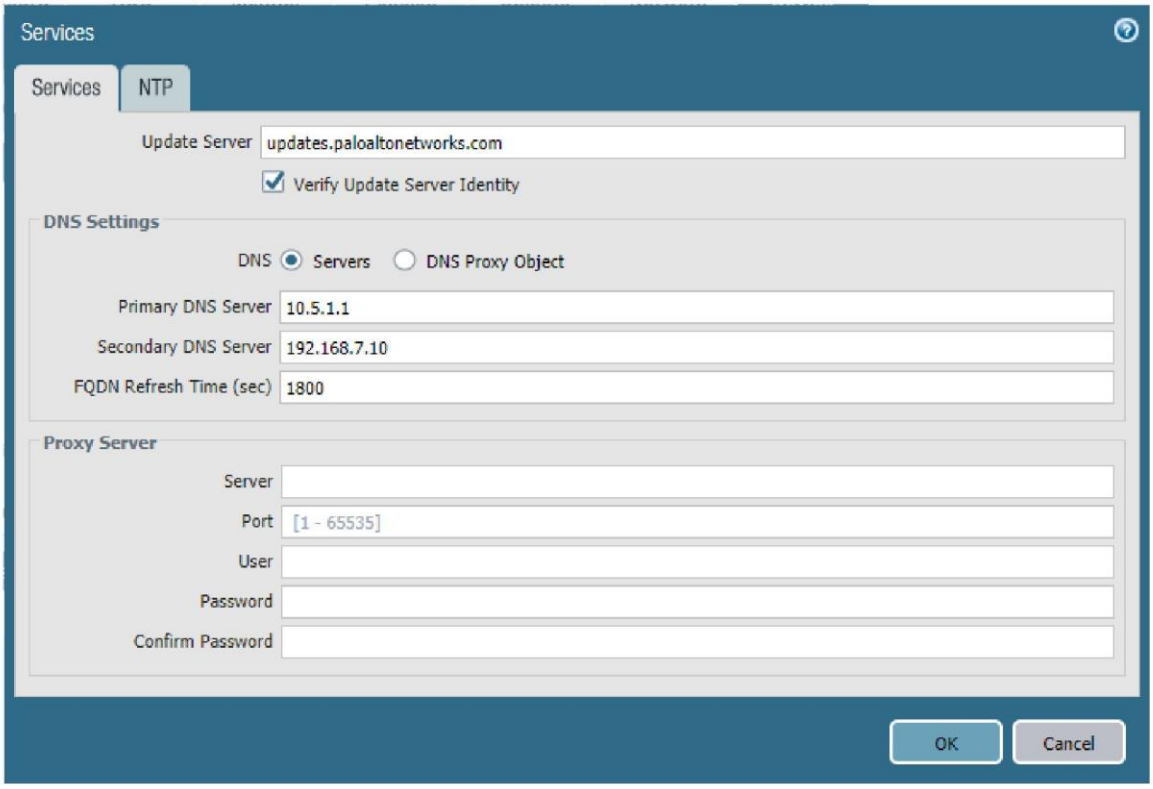
2.5.2.2. 2.5.2.3. KONFIGUROWANIE SERWERA DNS I PROTOKOŁU NTP

1. W portalu **Palo Alto Networks Portal** wybierz kolejno opcje **Device** (Urządzenie) > **Setup** (Konfiguracja) > **Services** (Usługi).
2. Na karcie **Services** (Usługi) kliknij ikonę koła zębatego.



Rysunek 2-32 Konfiguracja usług Palo Alto Networks

3. Na karcie **Services** (Usługi) > **Services** (Usługi):
    a. W polu **Primary DNS Server** (Główny serwer DNS) wprowadź adres IP głównego serwera DNS.
    b. W polu **Secondary DNS Server** (Pomocniczy serwer DNS) wprowadź adres IP pomocniczego serwera DNS, jeśli taki istnieje.
4. Wybierz kartę **NTP**.



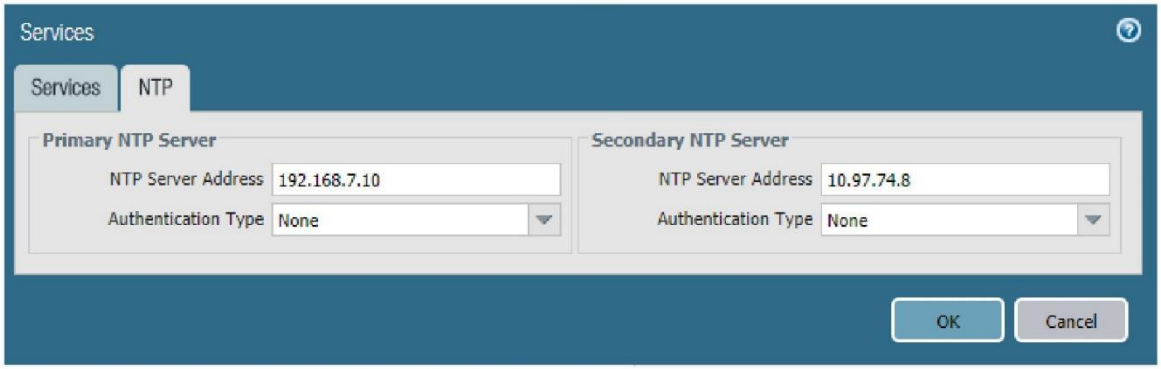
Rysunek 2-33 Konfiguracja serwera DNS

5. Na karcie **NTP**:

    a. W części **Primary NTP Server** (Główny serwer NTP) w polu **NTP Server Address** (Adres serwera NTP) wprowadź adres IP głównego serwera NTP, który ma być używany.

    b. W części **Secondary NTP Server** (Pomocniczy serwer NTP) w polu **NTP Server Address** (Adres serwera NTP) wprowadź adres IP pomocniczego serwera NTP, który ma być używany (jeśli istnieje).

6. Kliknij przycisk **OK**.



Rysunek 2-34 Konfiguracja serwera NTP

2.5.3. KONFIGURACJA INTERFEJSÓW I STREF URZĄDZENIA PALO ALTO NETWORKS

Zapora sieciowa Palo Alto Networks model PA-220 jest wyposażona w osiem interfejsów, które można skonfigurować jako zaufane (wewnętrzne) lub niezaufane (zewnętrzne). W tym punkcie opisano sposób tworzenia strefy i przypisywania do niej interfejsu.

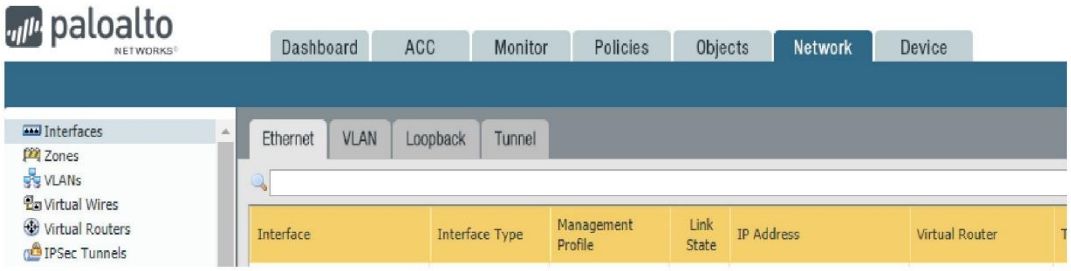
2.5.3.1. TWORZENIE INTERFEJSÓW I ADRESÓW ETHERNET

W naszym przykładowym wdrożeniu wykorzystano trzy interfejsy:

- LAN: sieć LAN firmy Orvilia, która obsługuje strony i pocztę w intranecie.
- DMZ: podsieć DMZ firmy Orvilia, w której znajduje się system MobileIron Core i MobileIron Sentry.
- WAN: zapewnia dostęp do Internetu i jest interfejsem przychodzącym dla bezpiecznych połączeń (SSL) VPN.

Aby utworzyć i skonfigurować interfejsy Ethernet:

1. Przejdź do portalu **Palo Alto Networks** i użyj kolejno opcji > **Network** (Sieć) > **Ethernet** > **Interfaces** (Interfejsy) > **Ethernet**.



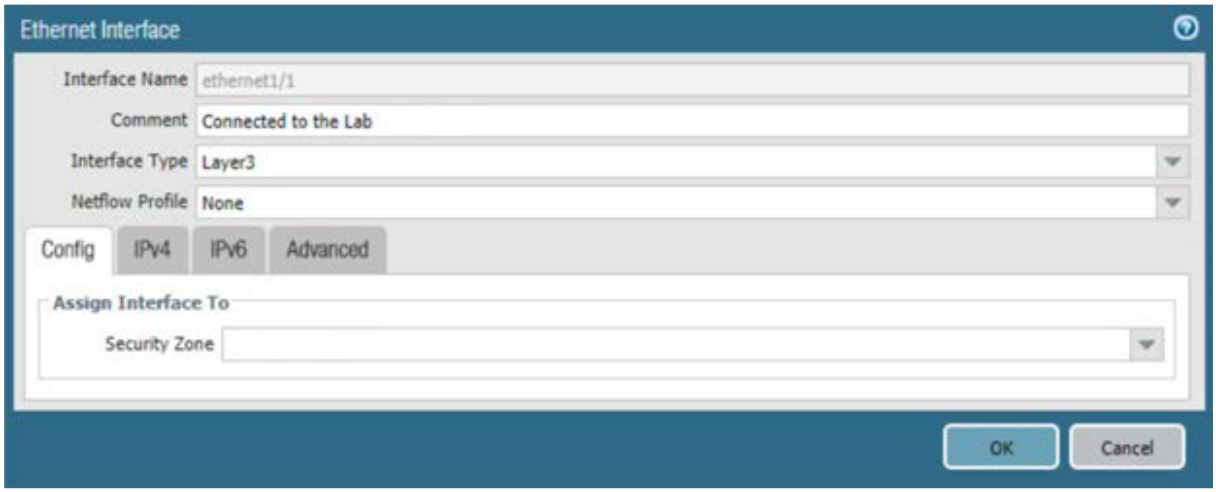
Rysunek 2-35 Interfejsy Ethernet

2. Na karcie Ethernet wybierz nazwę interfejsu do skonfigurowania. Pojawi się okno dialogowe **Ethernet Interface** (Interfejs Ethernet).

3. W oknie dialogowym **Ethernet Interface** (Interfejs Ethernet):

    a. W polu **Comment** (Komentarz) wprowadź opis tego interfejsu.

    b. Z menu rozwijanego **Interface Type** (Typ interfejsu) wybierz opcję **Layer3** (Warstwa3).



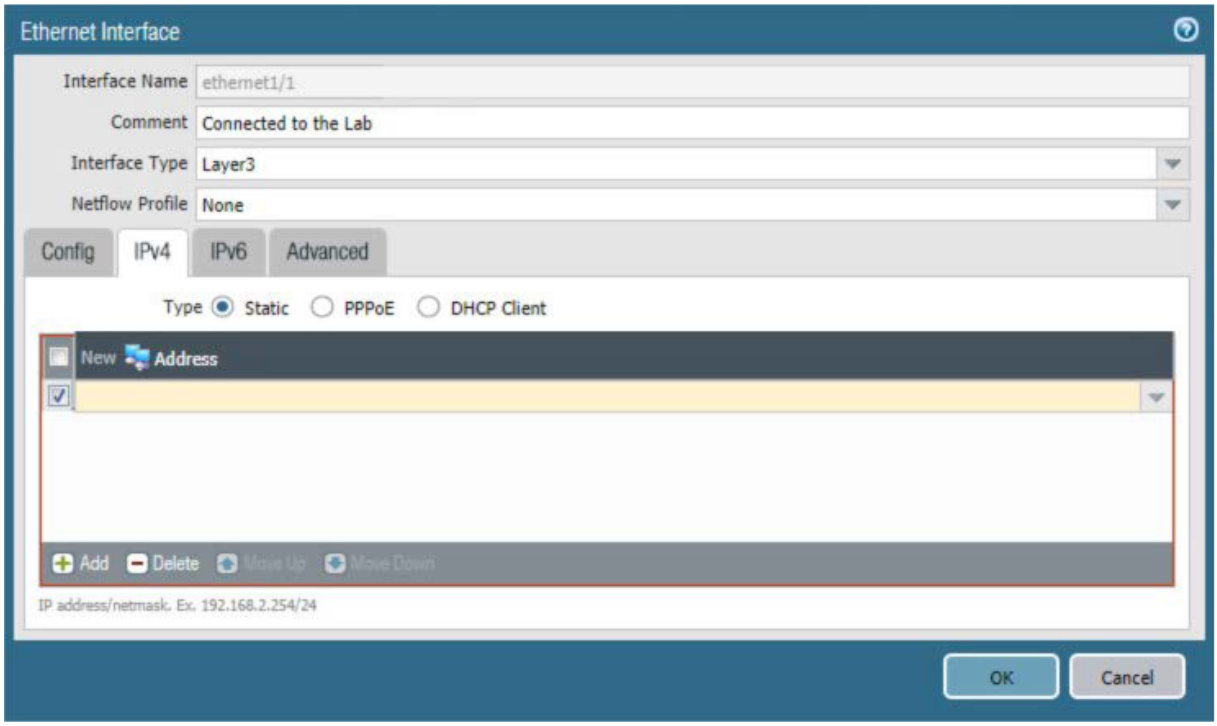
Rysunek 2-36 Konfiguracja interfejsu Ethernet

    c. Wybierz kartę **IPv4**.

    d. Na karcie **IPv4**:

        i. W polu listy adresów IP kliknij przycisk **Add** (Dodaj). Na liście pojawi się pusta pozycja.

ii. W pustej pozycji listy wybierz opcję **New Address** (Nowy adres). Pojawi się okno dialogowe **Address** (Adres).



Rysunek 2-37 Konfiguracja protokołu IPv4 interfejsu WAN

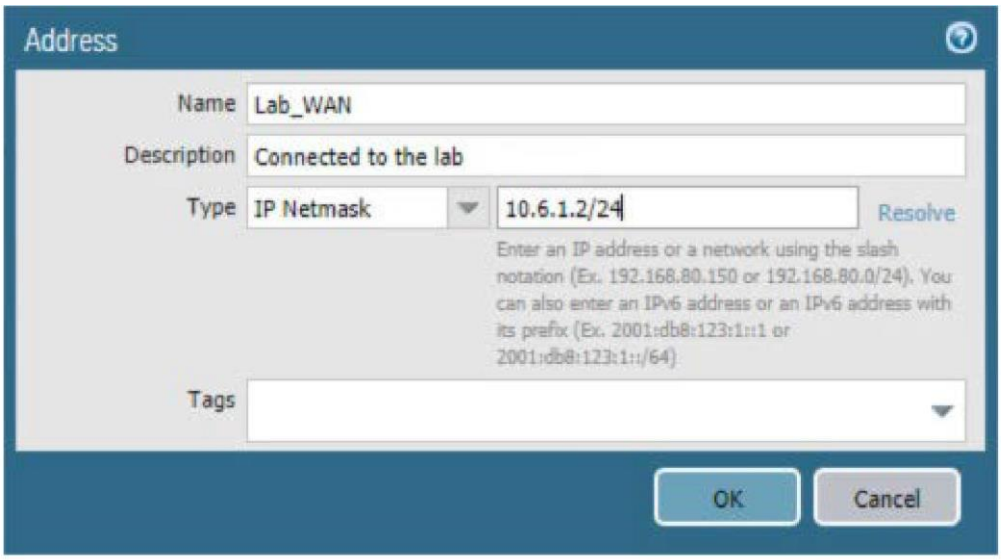
iii. W oknie dialogowym **Address** (Adres):

1) W polu **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi identyfikację tego adresu.

2) W polu **Description** (Opis) wprowadź tekst opisujący przeznaczenie tego adresu.

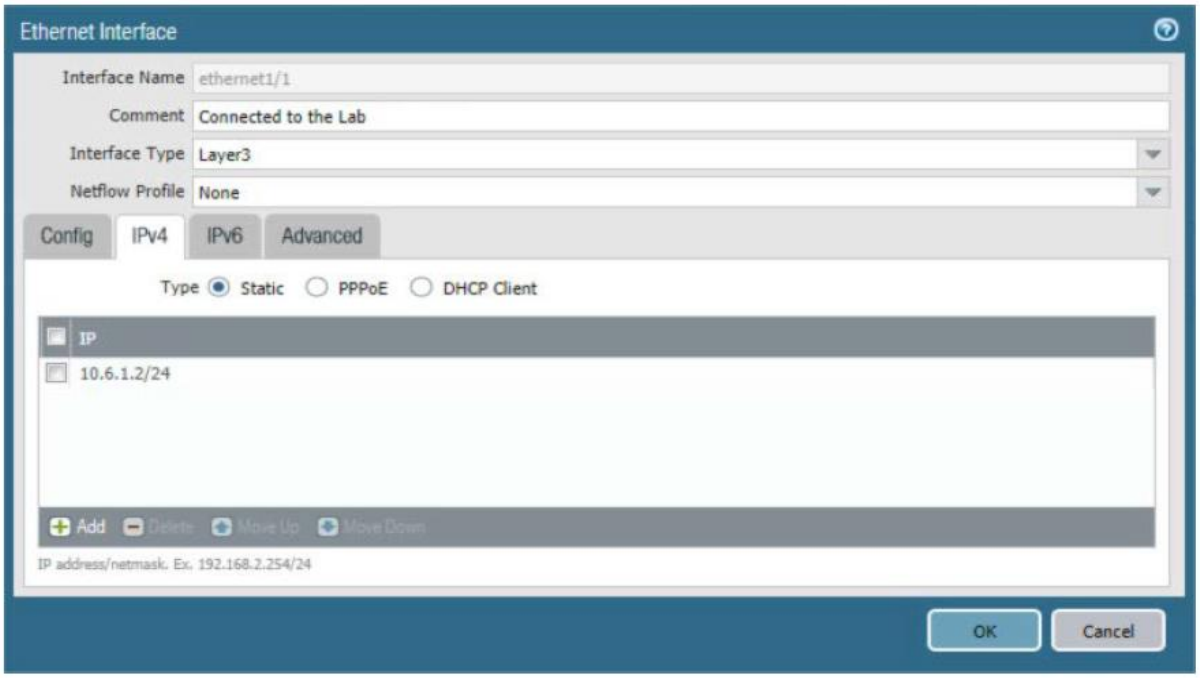
3) W polu bez nazwy znajdującym się obok rozwijanego menu **Type** (Typ) wprowadź adres IPv4, który będzie używany przez ten interfejs w notacji **Classless Inter-Domain Routing** (bezklasowy routing międzydomenowy). W tym przykładzie dla interfejsu WAN w naszym środowisku laboratoryjnym użyto adresu **10.6.1.2/24**.

4) Kliknij przycisk **OK**.



Rysunek 2-38 Konfiguracja adresu IP interfejsu WAN

e. Wprowadzony adres powinien pojawić się jako pozycja w polu listy adresów IP. Kliknij przycisk **OK**, aby zamknąć okno dialogowe **Address** (Adres).



Rysunek 2-39 Ukończona konfiguracja interfejsu WAN

4. Kliknij przycisk **OK**.

5. Powtórz kroki 2 i 3 dla każdego z dodatkowych interfejsów Ethernet/Layer3.

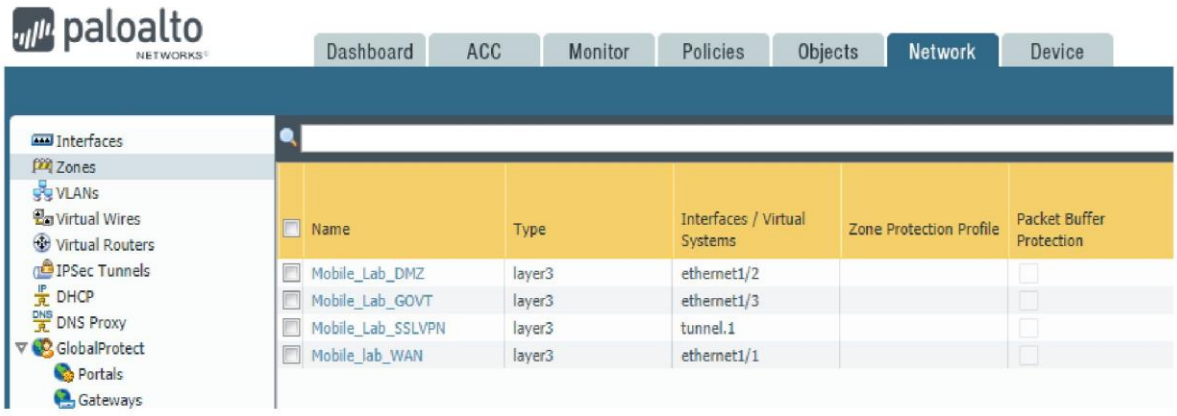
2.5.3.2. TWORZENIE STREF BEZPIECZEŃSTWA

Strefa bezpieczeństwa PA[9] to zbiór obejmujący jeden lub wiele interfejsów, dla których obowiązują te same reguły bezpieczeństwa. Na potrzeby tego projektu skonfigurowano cztery różne strefy:

- *Mobile_Lab_GOVT*: wewnętrzny (zaufany) interfejs łączący się z segmentem rządowym (GOVT).
- *Mobile_Lab_DMZ*: wewnętrzny (zaufany) interfejs łączący się z segmentem DMZ.
- *Mobile_Lab_WAN*: zewnętrzny (niezaufany) interfejs zezwalający na zaufane połączenia przychodzące (np. z usługą w chmurze Lookout) z niezaufanego Internetu i umożliwiający dostęp do Internetu urządzeniom lokalnym.
- *Mobile_Lab_SSLVPN*: zewnętrzny (niezaufany) interfejs dla połączeń VPN z zaufanych urządzeń mobilnych pochodzących z niezaufanych sieci (np. publicznych sieci Wi-Fi).

Aby skonfigurować każdą ze stref:

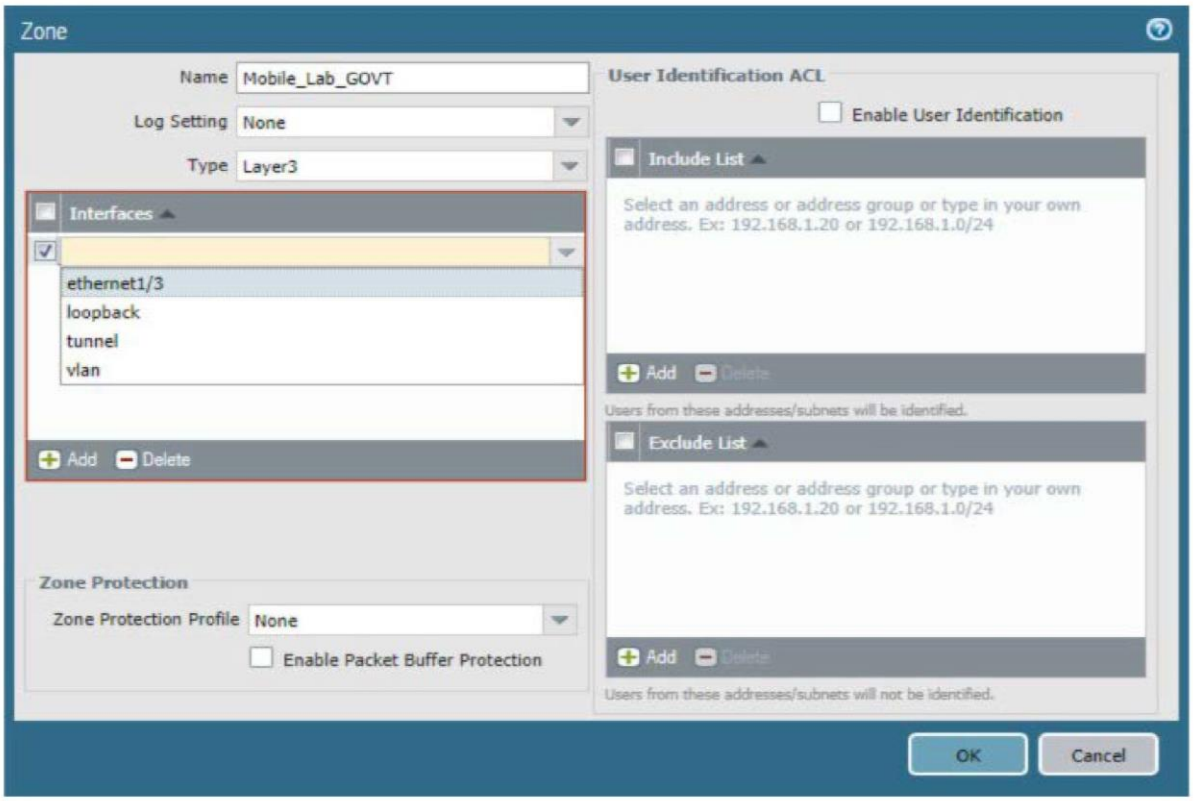
1. Przejdź do portalu **Palo Alto Networks** i wybierz kolejno opcje > **Network** (Sieć) > **Zones** (Strefy).



Rysunek 2-40 Lista stref bezpieczeństwa

[9] Palo Alto

2. W okienku **Zones** (Strefy) kliknij przycisk **Add** (Dodaj). Zostanie otwarta strona **Zones** (Strefy).
3. Na stronie **Zones** (Strefy):
   a. W polu **Name** (Nazwa) wprowadź unikalną nazwę dla strefy.
   b. Z menu rozwijanego **Type** (Typ) wybierz opcję **Layer 3** (Warstwa 3).
   c. W części **Interfaces** (Interfejsy) kliknij przycisk **Add** (Dodaj). Pojawi się menu rozwijane bez nazwy.
   d. Z rozwijanego menu wybierz interfejs, który chcesz przypisać do danej strefy. W tym przykładzie wybrano interfejs **ethernet 1/3**, który jest powiązany z interfejsem LAN.
   e. Kliknij przycisk **OK**.



Rysunek 2-41 Konfiguracja strefy bezpieczeństwa interfejsu LAN

   f. Powtórz krok b dla każdej strefy.

2.5.4. KONFIGUROWANIE ROUTERA

Urządzenie Palo Alto Networks używa wirtualnego routera do emulowania fizycznej łączności między interfejsami w różnych strefach. Aby zezwolić systemom na dostęp do systemów w innych strefach, w ramach poniższych kroków należy utworzyć router wirtualny i dodać do niego interfejsy. Router określa również, który z tych interfejsów będzie działał jako lokalna brama do Internetu.

1. W portalu **Palo Alto Networks** wybierz kolejno opcje **Network** (Sieć) > **Virtual Routers** (Routery wirtualne).
2. Poniżej okienka szczegółów kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **Virtual Router** (Router wirtualny).
3. W formularzu **Virtual Router** (Router wirtualny), na karcie **Router Settings** (Ustawienia routera):
    a. W polu **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi identyfikację tego routera.
    b. Na karcie **Router Settings** (Ustawienia routera) > **General** (Ogólne):
        i. Pod polem listy **Interfaces** (Interfejsy) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.
        ii. Z rozwijanego menu nowej pozycji na liście wybierz istniejący interfejs.
        iii. Powtórz **kroki 3a** i **3b**, aby dodać wszystkie istniejące interfejsy do tego routera.
4. Wybierz kartę **Static Routes** (Trasy statyczne).
5. Na karcie **Static Routes** (Trasy statyczne) **> IPv4**:
    a. Poniżej pola listy kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **Virtual Router - Static Route - IPv4** (Router wirtualny - trasa statyczna - IPv4).
    b. W formularzu **Virtual Router - Static Route - IPv4** (Router wirtualny - trasa statyczna - IPv4):

i. W polu **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi identyfikację tej trasy.

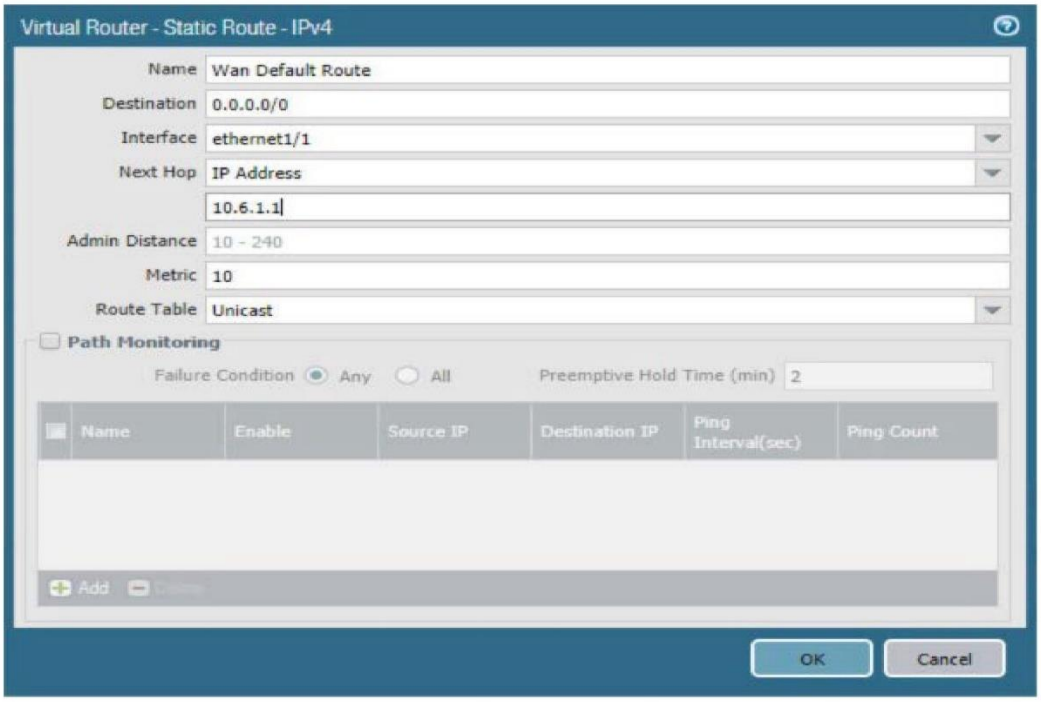
ii. W polu **Destination** (Lokalizacja docelowa) wpisz wartość 0.0.0.0/0.

iii. Z menu rozwijanego **Interface** (Interfejs) wybierz interfejs zapewniający dostęp do Internetu.

iv. Z menu rozwijanego **Next Hop** (Następny przeskok) wybierz opcję **IP Address** (Adres IP).

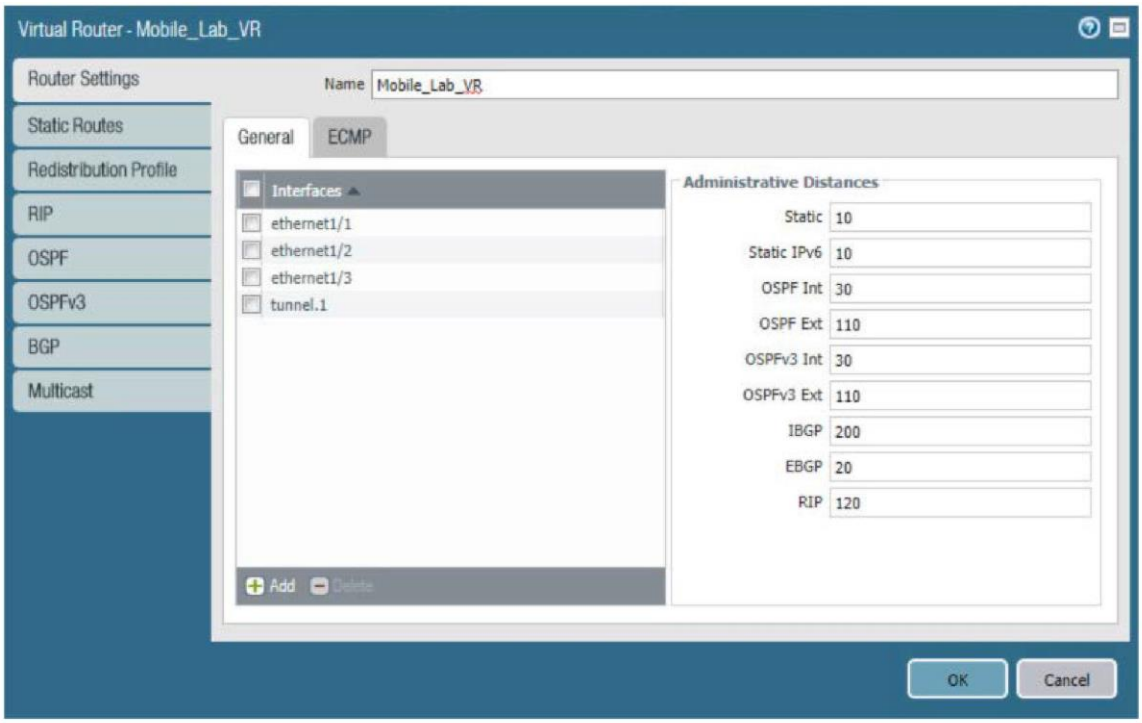
v. W polu poniżej menu **Next Hop** (Następny przeskok) wprowadź adres IP bramy zapewniającej dostęp do Internetu.

vi. Kliknij przycisk **OK**.



Rysunek 2-42 Konfiguracja routera wirtualnego

6. Kliknij przycisk **OK**.



Rysunek 2-43 Ustawienia ogólne routera wirtualnego

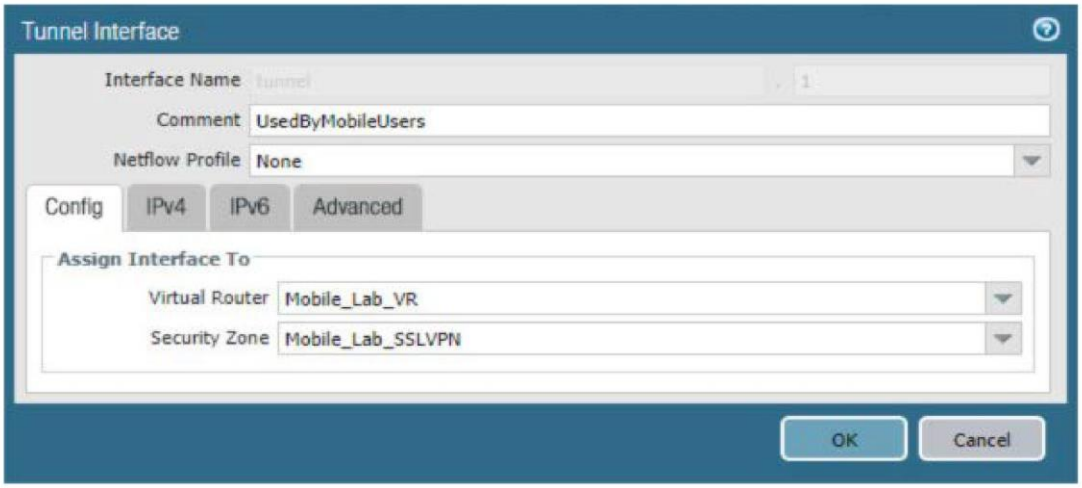
2.5.5. KONFIGURACJA INTERFEJSU TUNELOWEGO

Sieć SSL VPN wykorzystuje interfejs tunelowy do zabezpieczenia ruchu ze strefy zewnętrznej do strefy wewnętrznej, w której utrzymywane są zasoby organizacji dostępne dla użytkowników mobilnych. Aby skonfigurować interfejs tunelowy:

1. Przejdź do portalu **Palo Alto Networks** i wybierz kolejno opcje > **Network** (Sieć) > **Ethernet** > **Interfaces** (Interfejsy) > **Tunnel** (Tunel).
2. Poniżej okienka szczegółów kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **Tunnel Interface** (Interfejs tunelowy).
3. W formularzu **Tunnel Interface** (Interfejs tunelowy) na karcie **Config** (Konfiguracja):
    a. W części **Assign Interface To** (Przypisz interfejs do):
        i. Z menu rozwijanego **Virtual Router** (Router wirtualny) wybierz router wirtualny utworzony w poprzednim punkcie.

ii. Z menu rozwijanego **Security Zone** (Strefa bezpieczeństwa) wybierz strefę bezpieczeństwa utworzoną dla sieci SSL VPN.

b. Kliknij przycisk **OK**.



Rysunek 2-44 Interfejs tunelowy SSL VPN

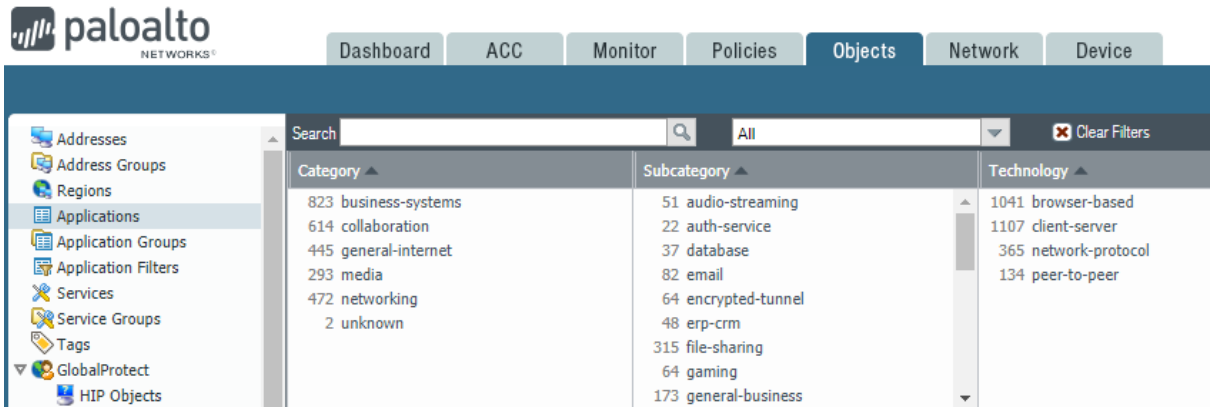
2.5.6. KONFIGURACJA APLIKACJI I ZASAD BEZPIECZEŃSTWA

Zasady bezpieczeństwa działają podobnie do reguł zapory sieciowej. Umożliwiają one blokowanie lub zezwalanie na ruch między zdefiniowanymi strefami określonymi przez źródło, lokalizację docelową i aplikacje (kontekstowo, obiekty Palo Alto Networks definiują protokoły sieciowe i porty). Urządzenie Palo Alto Networks ma wbudowane aplikacje dla dużej liczby standardowych i dobrze znanych protokołów i portów (np. LDAP i Secure Shell), ale zdefiniowaliśmy niestandardowe aplikacje dla ruchu specyficznego dla systemu MobileIron.

2.5.6.1. KONFIGUROWANIE APLIKACJI

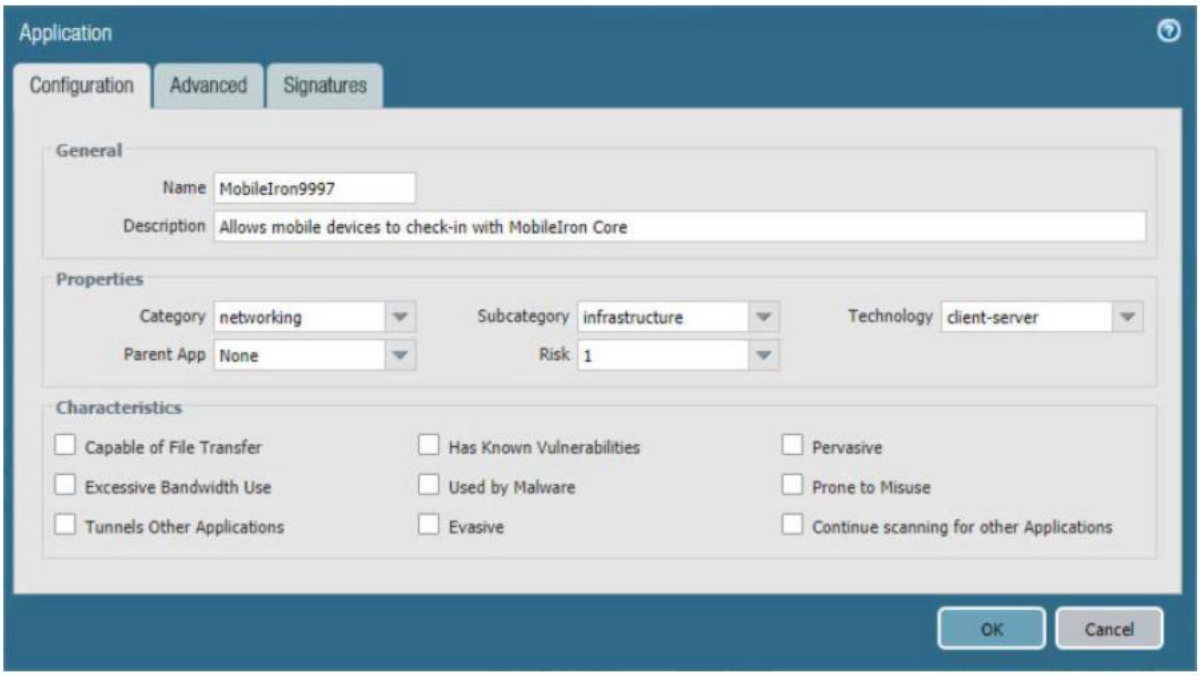
W poniższych krokach zostanie utworzona aplikacja:

1. W portalu **Palo Alto Networks** wybierz kolejno opcje **Objects** (Obiekty) > **Applications** (Aplikacje).



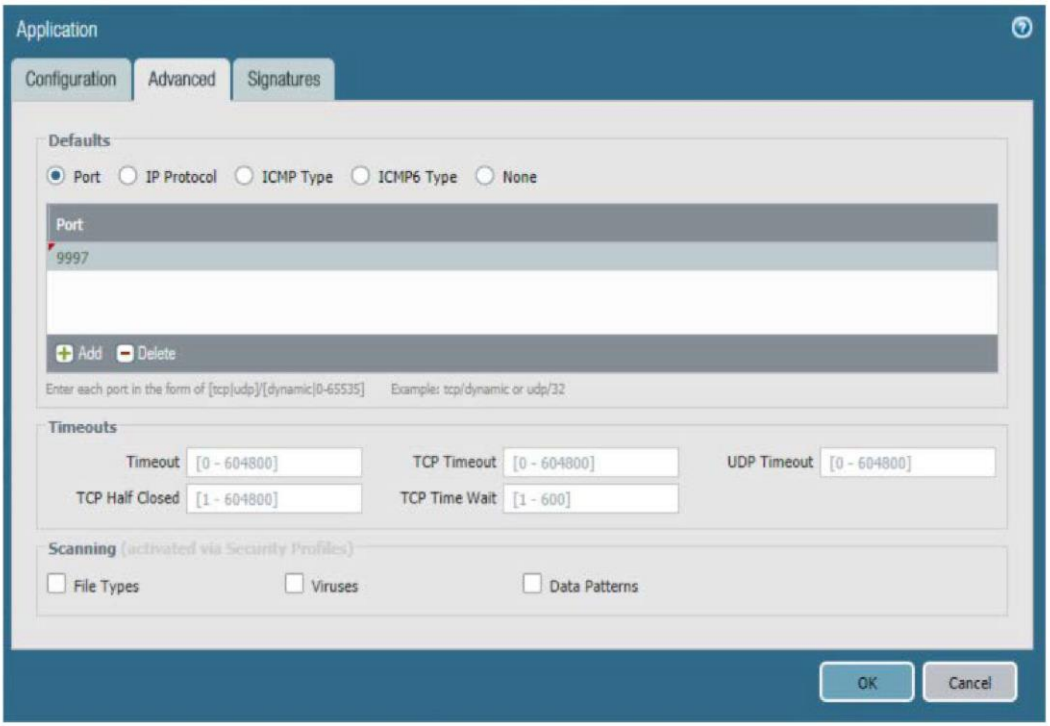
Rysunek 2-45 Kategorie aplikacji

2. Na ekranie **Applications** (Aplikacje):
3. Kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **Application** (Aplikacja).
4. Na ekranie **Application** (Aplikacja) > **Configuration** (Konfiguracja):
    a. W polu **General** (Ogólne) > **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi identyfikację tej aplikacji.
    b. W polu **General** (Ogólne) > **Description** (Opis) wprowadź tekst opisujący przeznaczenie tej aplikacji.
    c. Z menu rozwijanego **Properties** (Właściwości) > **Category** (Kategoria) wybierz kategorię odpowiednią dla danego środowiska. W naszej przykładowej implementacji użyto kategorii **networking** (sieciowa).
    d. Z menu rozwijanego **Properties** (Właściwości) > **Subcategory** (Podkategoria) wybierz podkategorię odpowiednią dla danego środowiska. W naszej przykładowej implementacji użyto podkategorii **infrastructure** (infrastruktura).
    e. Z menu rozwijanego **Properties** (Właściwości) > **Technology** (Technologia) wybierz technologię odpowiednią dla danego środowiska. W naszej przykładowej implementacji użyto technologii **client-server** (klient-serwer).



Rysunek 2-46 Konfiguracja aplikacji Palo Alto Networks w systemie MobileIron

5. Wybierz kartę **Advanced** (Zaawansowane).
6. Na ekranie **Application** (Aplikacja) > **Advanced** (Zaawansowane):
   a. Wybierz opcję **Defaults** (Domyślne) > **Port**.
   b. W polu listy Porty kliknij przycisk **Add** (Dodaj). Na liście pojawi się pusta pozycja.
   c. W pustej pozycji listy wprowadź numer portu używany przez aplikację. W tym przykładzie użyto numeru **9997**.
7. Kliknij przycisk **OK**.



Rysunek 2-47 Konfiguracja portu aplikacji MobileIron

8. Powtórz kroki od 2 do 7 z następującymi modyfikacjami, aby utworzyć aplikację dla konsoli administracyjnej systemu MobileIron Core:

    a. W polu **Configuration** (Konfiguracja) > **General** (Ogólne) > **Name** (Nazwa) należy wprowadzić **MobileIron8443**.

    b. W polu **Configuration** (Konfiguracja) > **Properties** (Właściwości) > **Category** (Kategoria) należy wybrać **business-systems** (systemy biznesowe).

    c. W polu **Configuration** (Konfiguracja) > **Properties** (Właściwości) > **Subcategory** (Podkategoria) należy wybrać **management** (zarządzanie).

    d. W polu **Advanced** (Zaawansowane) > **Defaults** (Domyślne) > **Port** należy wprowadzić 8443.

2.5.6.2. KONFIGURACJA ZASAD BEZPIECZEŃSTWA

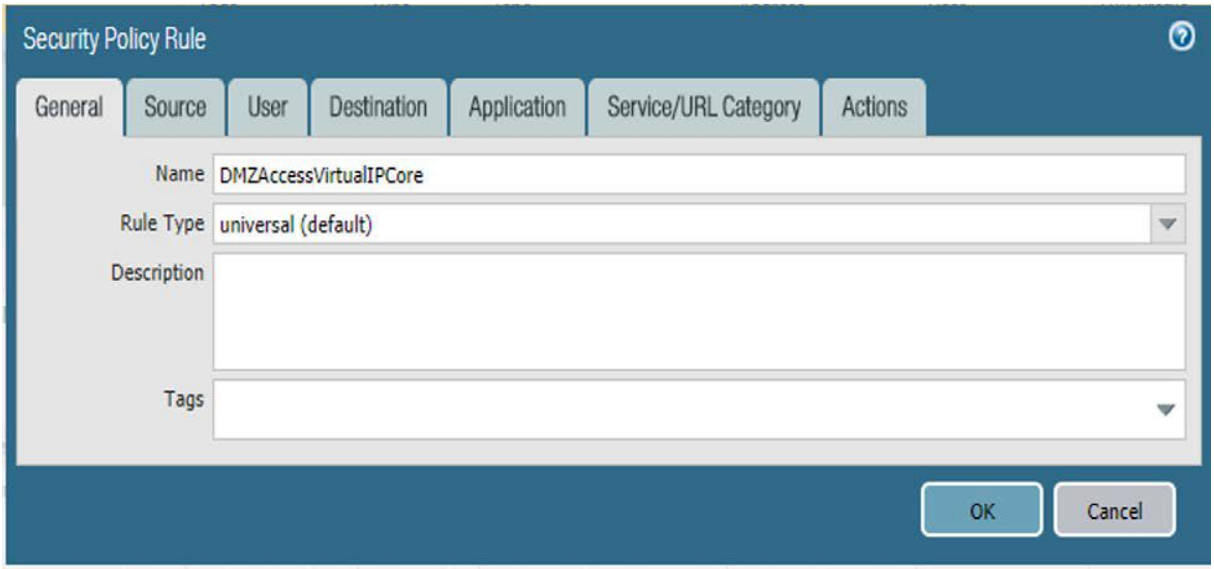
Zasady bezpieczeństwa zezwalają lub wyraźnie odrzucają komunikację wewnątrz, pomiędzy lub (zewnętrznie) do lub ze stref Palo Alto Networks. W przypadku tej

przykładowej implementacji utworzono kilka zasad bezpieczeństwa w celu umożliwienia komunikacji z innym komponentami architektury. W pierwszym podpunkcie opisano kroki tworzenia danej zasady bezpieczeństwa. W drugim podpunkcie znajduje się tabela zawierająca zasady bezpieczeństwa, których użyliśmy. Zasady te należy dostosować do nazw hostów i adresów IP specyficznych dla danej infrastruktury sieciowej.

2.5.6.2.1. TWORZENIE ZASAD BEZPIECZEŃSTWA

Aby utworzyć zasadę bezpieczeństwa:

1. W portalu **Palo Alto Networks** wybierz kolejno opcje **Policies** (Zasady) > **Security** (Bezpieczeństwo).
2. Kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **Security Policy Rule** (Reguła bezpieczeństwa).
3. W formularzu **Security Policy Rule** (Reguła bezpieczeństwa):
    a. W polu **Name** (Nazwa) wprowadź unikalną nazwę dla tej reguły bezpieczeństwa.
    b. Z menu rozwijanego **Rule Type** (Typ reguły) wybierz zakres reguły, postępując zgodnie z instrukcjami zawartymi w dokumentacji Palo Alto Networks dotyczącej tworzenia reguł zapory sieciowej.



Rysunek 2-48 Konfiguracja reguły zapory sieciowej w systemie MobileIron dla dostępu DMZ

4. Wybierz kartę **Source** (Źródło).

5. Na karcie **Source** (Źródło):

   a. Jeśli reguła bezpieczeństwa dotyczy określonej strefy źródłowej:

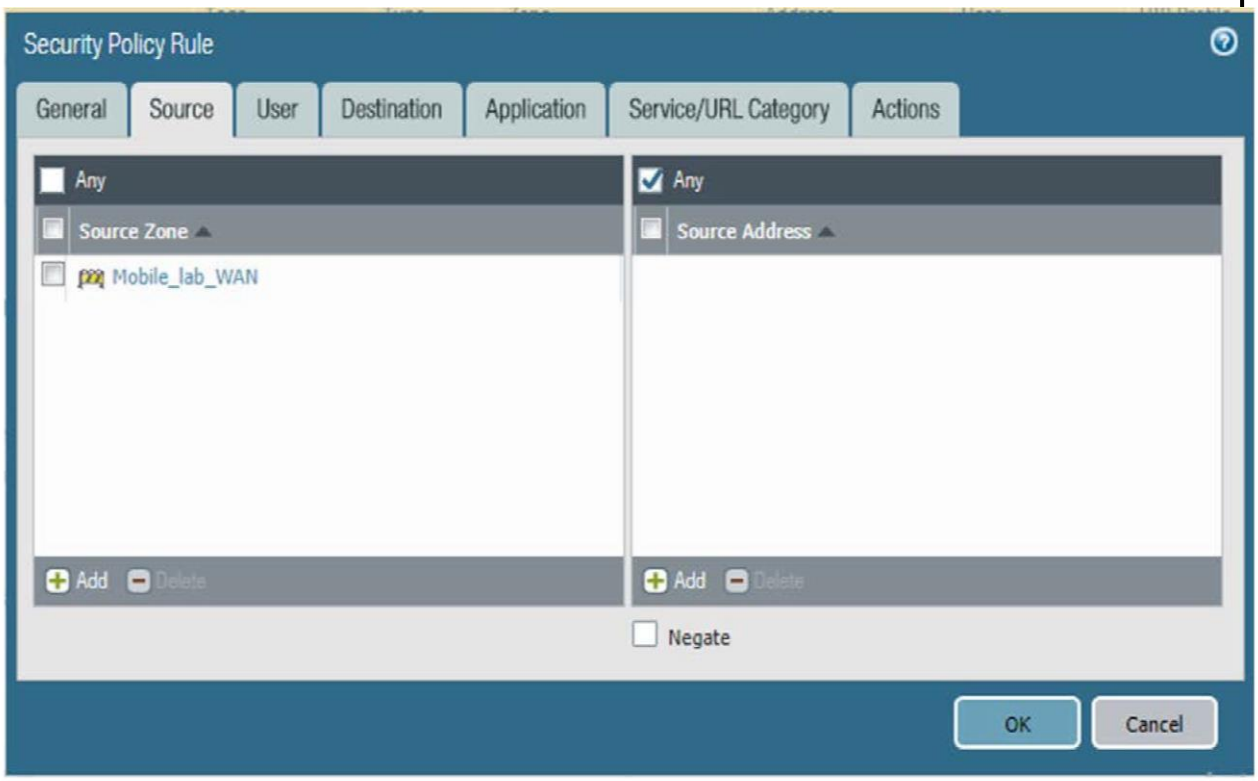
      i. Pod polem listy **Source Zone** (Strefa źródłowa) kliknij przycisk **Add** (Dodaj). W polu listy pojawi się nowy wpis.

      ii. W nowej pozycji na liście wybierz strefę źródłową dla tej reguły.

   b. Jeśli reguła dotyczy tylko określonych źródłowych adresów IP:

      i. Pod polem listy **Source Address** (Adres źródłowy) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.

      ii. W nowej pozycji na liście wybierz adres źródłowy dla tej reguły.



Rysunek 2-49 Konfiguracja reguły bezpieczeństwa strefy źródłowej w systemie MobileIron dla dostępu DMZ

6. Wybierz kartę **Destination** (Lokalizacja docelowa).

7. Na karcie **Destination** (Lokalizacja docelowa):

    a. Jeśli reguła bezpieczeństwa dotyczy określonej strefy docelowej:

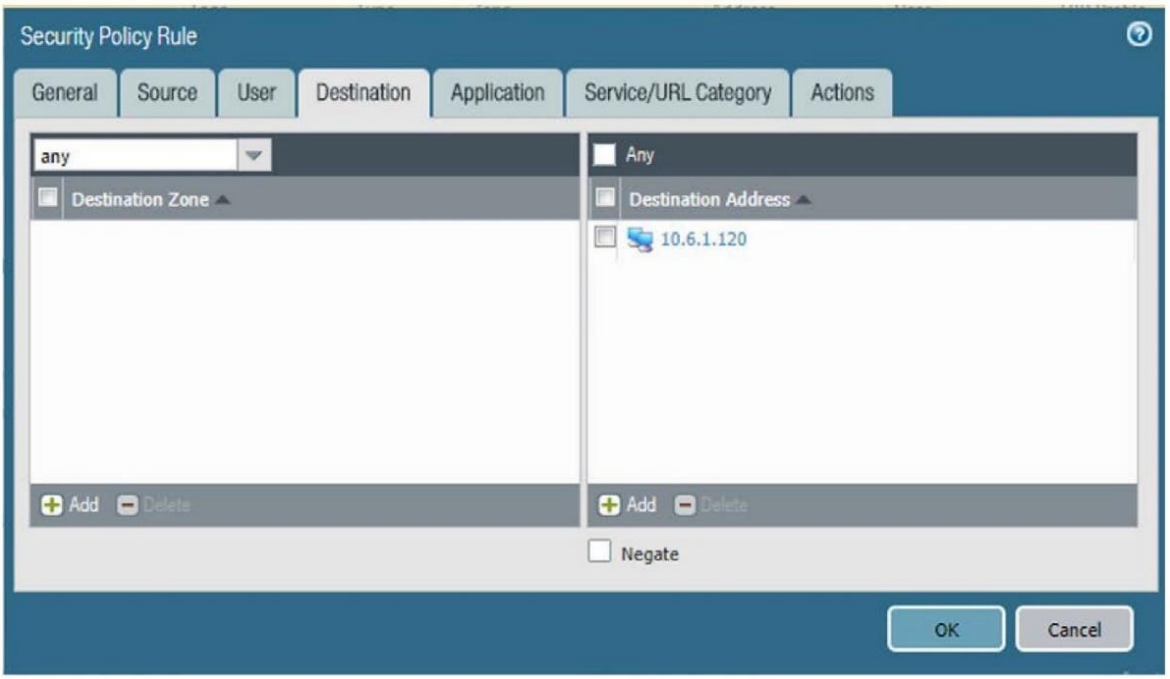
        i. Pod polem listy **Destination Zone** (Strefa docelowa) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.

        ii. W nowej pozycji na liście **Destination Zone** (Strefa docelowa) wybierz strefę docelową dla tej reguły.

    b. Jeśli reguła dotyczy tylko określonych docelowych adresów IP:

        i. Pod polem listy **Destination Address** (Adres docelowy) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.

        ii. W nowej pozycji na liście wybierz adres docelowy dla tej reguły.



Rysunek 2-50 Konfiguracja reguły bezpieczeństwa adresu docelowego w systemie MobileIron dla dostępu DMZ

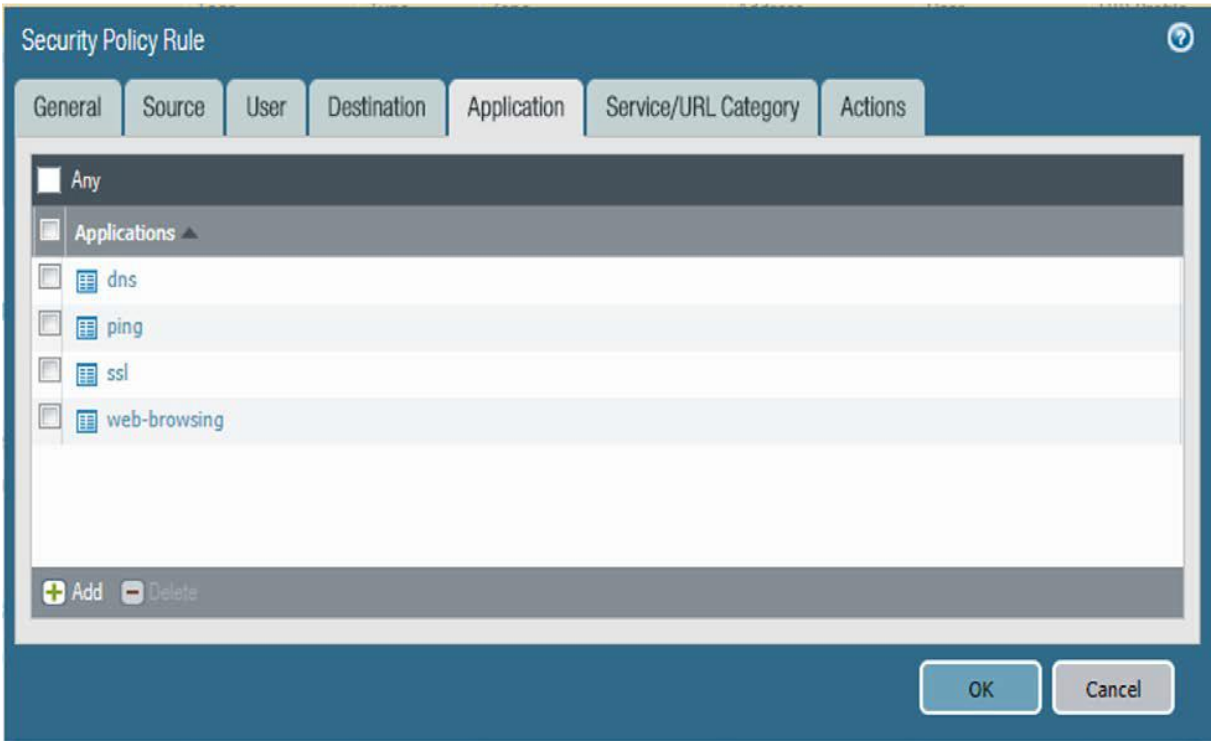
8. Wybierz kartę **Application** (Aplikacja).

9. Na karcie **Application** (Aplikacja):

a. Pod polem listy **Applications** (Aplikacje) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.

b. W nowej pozycji na liście **Applications** (Aplikacje) wybierz aplikację obsługującą kombinację protokołu i portu dla ruchu, który ma być kontrolowany.

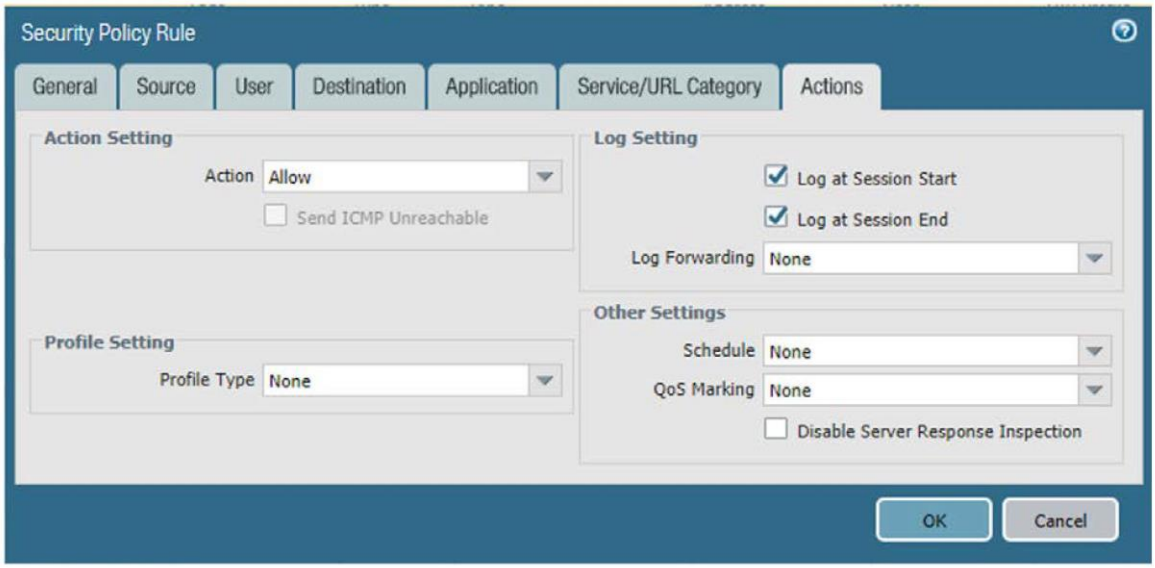
c. Powtórz kroki 9a i 9b dla każdej aplikacji korzystającej z tego samego źródła i lokalizacji docelowej, dla której ruch również byłby dozwolony lub wyraźnie zabroniony (jeśli zezwala na niego bardziej liberalna reguła bezpieczeństwa).



Rysunek 2-51 Konfiguracja reguły bezpieczeństwa protokołu aplikacji w systemie MobileIron dla dostępu DMZ

10. Wybierz kartę **Actions** (Akcje).

11. Na karcie **Actions** (Akcje): Jeśli ruch dozwolony przez bardziej liberalną regułę bezpieczeństwa nie ma być wyraźnie blokowany, należy upewnić się, że w menu rozwijanym **Action Setting** (Ustawienia akcji) > **Action** (Akcja) wybrano ustawienie **Allow** (Zezwalaj).



Rysunek 2-52 Konfiguracja reguły bezpieczeństwa akcji w systemie MobileIron dla dostępu DMZ

12. Kliknij przycisk **OK**.

2.5.6.2.2. WDROŻONE ZASADY BEZPIECZEŃSTWA

Wdrożone zasady bezpieczeństwa przedstawiono w tabeli 2-1, tabeli 2-2 i tabeli 2-3. Dla opcji konfiguracji, które nie zostały zaprezentowane, pozostawiono wartości domyślne.

Tabela 2-1 Wdrożone zasady bezpieczeństwa

Nazwa	Znaczniki	Typ	Strefa źródłowa	Adres źródłowy
DMZAccessVirtualIPCore	brak	uniwersalny	Mobile_lab_WAN	dowolny
CoretoAppleSrvs	brak	uniwersalny	Mobile_Lab_DMZ	MI_Core
AdminAccessToMI	brak	międzystrefowy	Mobile_Lab_GOVT	MDS.govt.admin
AppthorityConnectorAccessToMI-Core	brak	międzystrefowy	Mobile_Lab_GOVT	govt.appthority
MICoreObtainDeviceCERT	brak	międzystrefowy	Mobile_Lab_DMZ	MI_Core
MICoreAccessDNS	brak	międzystrefowy	Mobile_Lab_DMZ	MI_Core
MICoreRelaySMSNotifications	brak	międzystrefowy	Mobile_Lab_DMZ	MI_Core
MICoreSyncLDAP	brak	międzystrefowy	Mobile_Lab_DMZ	MI_Core

Tabela 2-2 Wdrożone zasady bezpieczeństwa

Nazwa	Użytkownik źródłowy	Profil protokołu informacji o hoście źródłowym	Strefa docelowa	Adres docelowy
DMZAccessVirtualIPCore	dowolny	dowolny	dowolny	10.6.1.120
CoretoAppleSrvs	dowolny	dowolny	dowolny	17.0.0.0/8
AdminAccessToMI	dowolny	dowolny	Mobile_Lab_DMZ	MI_Core; MI_Sentry
AppthorityConnectorAccessToMI-Core	dowolny	dowolny	Mobile_Lab_DMZ	MI_Core
MICoreObtainDeviceCERT	dowolny	dowolny	Mobile_Lab_GOVT	SCEP_server
MICoreAccessDNS	dowolny	dowolny	Mobile_Lab_GOVT	DNS_Server
MICoreRelaySMSNotifications	dowolny	dowolny	Mobile_Lab_GOVT	SMTP_Relay
MICoreSyncLDAP	dowolny	dowolny	Mobile_Lab_GOVT	LDAP_Server

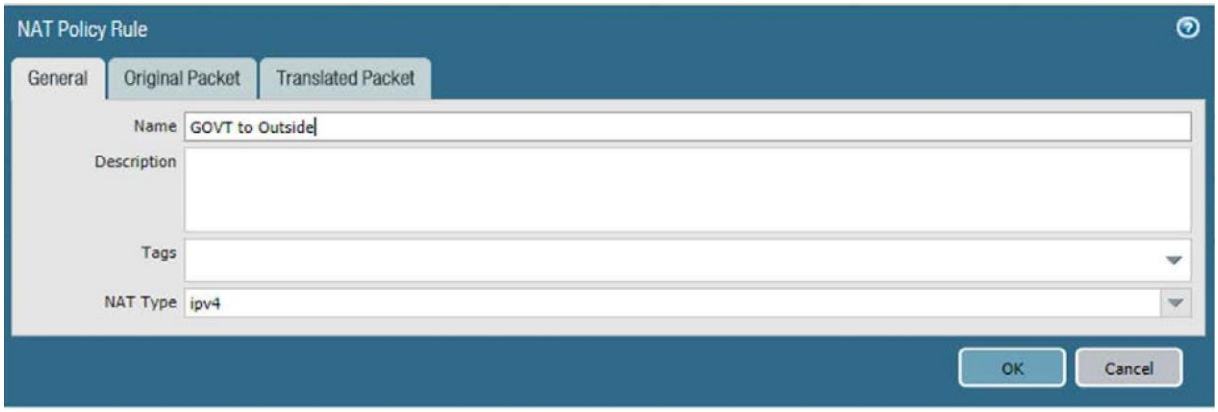
Tabela 2-3 Wdrożone zasady bezpieczeństwa

Nazwa	Aplikacja	Usługa	Akcja	Profil	Opcje
DMZAccessVirtualIPCore	dns;ping;ssl;web-browsing	dowolna	zezwól	brak	brak
CoretoAppleSrvs	dowolny	dowolna	zezwól	brak	brak
AdminAccessToMI	AdminAccessMI;ssh;ssl	dowolna	zezwól	brak	brak
AppthorityConnectorAccessToMI-Core	AdminAccessMI; ssl;web-browsing	dowolna	zezwól	brak	brak
MICoreObtainDeviceCERT	scep;web-browsing	application-default	zezwól	brak	brak
MICoreAccessDNS	dns	application-default	zezwól	brak	brak
MICoreRelaySMSNotifications	smtp	application-default	zezwól	brak	brak
MICoreSyncLDAP	ldap	application-default	zezwól	brak	brak

2.5.7. TRANSLACJA ADRESÓW SIECIOWYCH

Aby umożliwić komunikację z sieciami zewnętrznymi przez Internet, w konfiguracji urządzenia należy również uwzględnić reguły translacji adresów sieciowych (*ang. Network Address Translation – NAT*). Aby skonfigurować proces NAT:

1. W portalu **Palo Alto Networks** wybierz kolejno opcje **Policies** (Zasady) > **NAT.**
2. Poniżej okienka szczegółów kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **NAT Policy Rule** (Reguła NAT).
3. W formularzu **NAT Policy Rule** (Reguła NAT), na karcie **General** (Ogólne):
    a. W polu **Name** (Nazwa) wprowadź unikalną nazwę dla tej reguły NAT.
    b. Upewnij się, że w menu rozwijanym **NAT Type** (Typ NAT) wybrano opcję ipv4.



Rysunek 2-53 Reguła wychodzących procesów NAT

4. Wybierz kartę **Original Packet** (Oryginalny pakiet).
5. Na karcie **Original Packet** (Oryginalny pakiet):
    a. Pod polem listy **Source Zone** (Strefa źródłowa) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.
    b. W nowej pozycji na liście **Source Zone** (Strefa źródłowa) wybierz strefę odpowiadającą podsieci LAN. W tym przykładowym wdrożeniu jest to **Mobile_Lab_GOVT**.

c. Powtórz kroki 5a i 5b, aby dodać strefę odpowiadającą DMZ. W tym przykładowym wdrożeniu jest to Mobile_Lab_DMZ.

d. Powtórz kroki 5a i 5b, aby dodać strefę odpowiadającą sieci SSL VPN. W tym przykładowym wdrożeniu jest to **Mobile_Lab_SSLVPN**.

e. Z menu rozwijanego **Destination Zone** (Strefa docelowa) wybierz strefę odpowiadającą Internetowi. W tym przykładowym wdrożeniu jest to **Mobile_lab_WAN**.

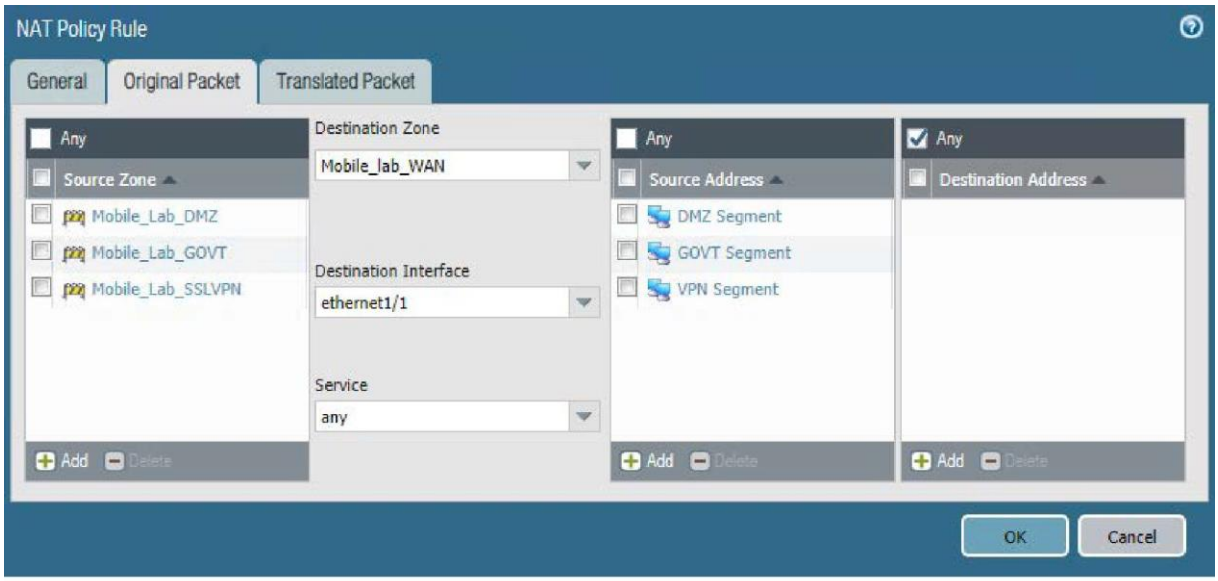
f. W polu **Destination Interface** (Interfejs docelowy) wybierz adapter, który jest fizycznie podłączony do tej samej podsieci, co brama internetowa. W tym przykładowym wdrożeniu jest to **ethernet1/1**.

g. Pod polem listy **Source Address** (Adres źródłowy) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.

h. W nowej pozycji na liście **Source Address** (Adres źródłowy) wybierz adres odpowiadający podsieci (zakresowi adresów IP) sieci LAN.

i. Powtórz kroki 5f i 5g, aby dodać adres odpowiadający podsieci DMZ.

j. Powtórz kroki 5f i 5g, aby dodać adres odpowiadający podsieci SSL VPN.



Rysunek 2-54 Konfiguracja oryginalnego pakietu wychodzących procesów NAT

6. Wybierz kartę **Translated Packet** (Pakiet po translacji).

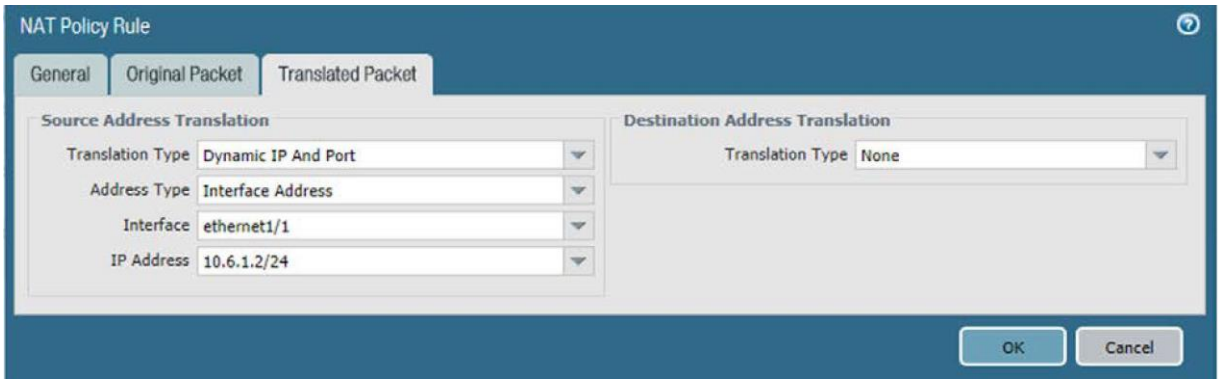
7. Na karcie **Translated Packet** (Pakiet po translacji), w obszarze **Source Address Translation** (Translacja adresów źródłowych):

    a. Z menu rozwijanego **Translation Type** (Typ translacji) wybierz opcję **Dynamic IP and Port** (Dynamiczny adres IP i port).

    b. Z menu rozwijanego **Address Type** (Typ adresu) wybierz opcję **Interface Address** (Adres interfejsu).

    c. Z menu rozwijanego **Interface** (Interfejs) wybierz ten sam interfejs, który został wybrany w kroku 5e.

    d. Z menu rozwijanego **IP Address** (Adres IP) wybierz adres IPv4 w tej samej podsieci co brama internetowa.



Rysunek 2-55 Konfiguracja pakietów translacji wychodzących procesów NAT

8. Kliknij przycisk **OK**.

2.5.8. KONFIGURACJA SIECI SSL VPN

Sieć SSL VPN umożliwia zdalnym użytkownikom urządzeń mobilnych tworzenie szyfrowanych połączeń z przedsiębiorstwem z niezaszyfrowanych sieci (np. publicznych hot spotów Wi-Fi).

2.5.8.1. KONFIGURACJA UWIERZYTELNIANIA UŻYTKOWNIKÓW KOŃCOWYCH

Kroki opisane poniżej umożliwiają przeprowadzenie integracji i konfiguracji związanych z identyfikacją i uwierzytelnianiem użytkowników mobilnych.

2.5.8.1.1. KONFIGURACJA PROFILU SERWERA

W poniższych krokach urządzenie jest integrowane z usługami Microsoft Active Directory Domain Services w celu zarządzania uprawnieniami użytkowników mobilnych przy użyciu grup i ról AD.

1. W portalu **Palo Alto Networks** wybierz kolejno opcje **Devices** (Urządzenia) > **Server Profiles** (Profile serwerów) > **LDAP**.
2. Poniżej okienka szczegółów kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **LDAP Server Profile** (Profil serwera LDAP).
3. W formularzu **LDAP Server Profile** (Profil serwera LDAP):
    a. W polu **Profile Name** (Nazwa profilu) wprowadź unikalną nazwę, która umożliwi identyfikację tego profilu.

b. Pod polem listy **Server List** (Lista serwerów) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.

c. Dla nowej pozycji w polu **Server List** (Lista serwerów):

   i. W kolumnie **Name** (Nazwa) wprowadź nazwę, która umożliwi identyfikację serwera.

   ii. W kolumnie **LDAP Server** (Serwer LDAP) wprowadź adres IP serwera LDAP.

   iii. Domyślna wartość w kolumnie **Port** to 389. Zmień ją, jeśli serwer LDAP komunikuje się przez port o innym numerze.

   iv. Powtórz kroki od 3ci do 3ciii dla każdego serwera LDAP, który ma być używany.

d. W obszarze **Server Settings** (Ustawienia serwera):

   i. Z menu rozwijanego **Type** (Typ) wybierz opcję **active-directory**.

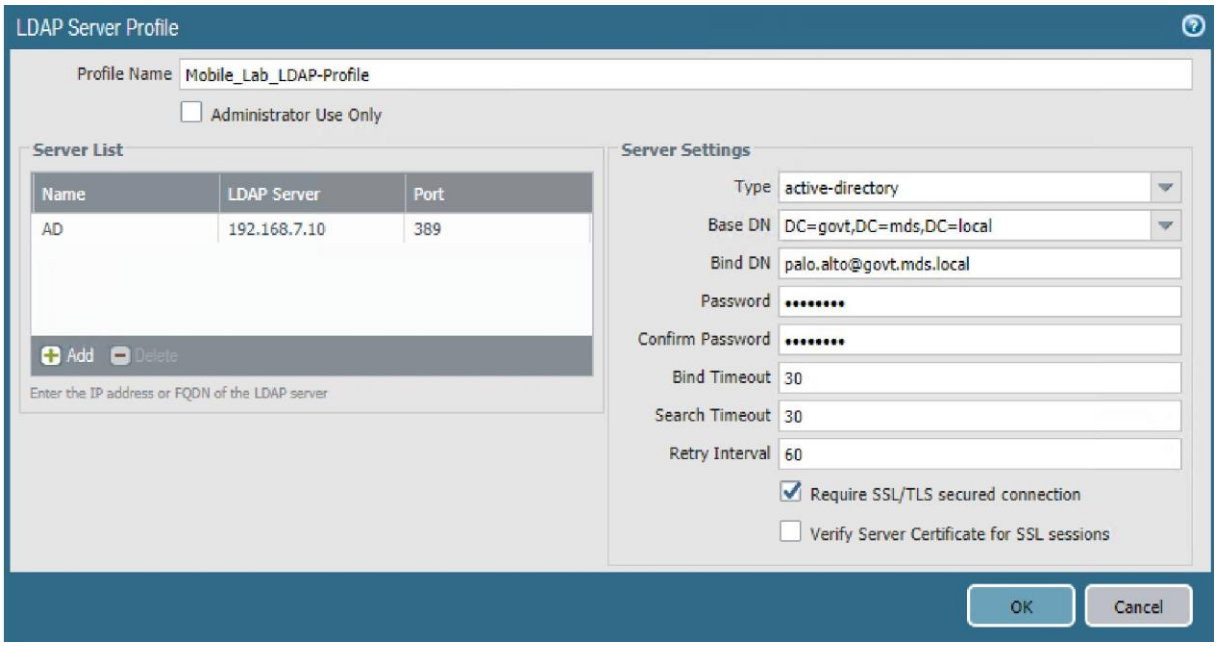
   ii. Z rozwijanego menu **Base DN** (Podstawowa nazwa DN) wybierz nazwę DN dla użytkowników domeny Active Directory, którzy będą korzystać z sieci SSL VPN.

   iii. W polu **Bind DN** (Nazwa DN powiązania) wprowadź konto użytkownika domeny Active Directory, które będzie uwierzytelniać się w LDAP w celu wykonywania zapytań.

   iv. W polu **Password** (Hasło) wprowadź hasło do konta użytkownika usługi Active Directory podanego w poprzednim kroku.

   v. W polu **Confirm Password** (Potwierdź hasło) wprowadź ponownie hasło podane w poprzednim kroku.

4. Kliknij przycisk **OK**.

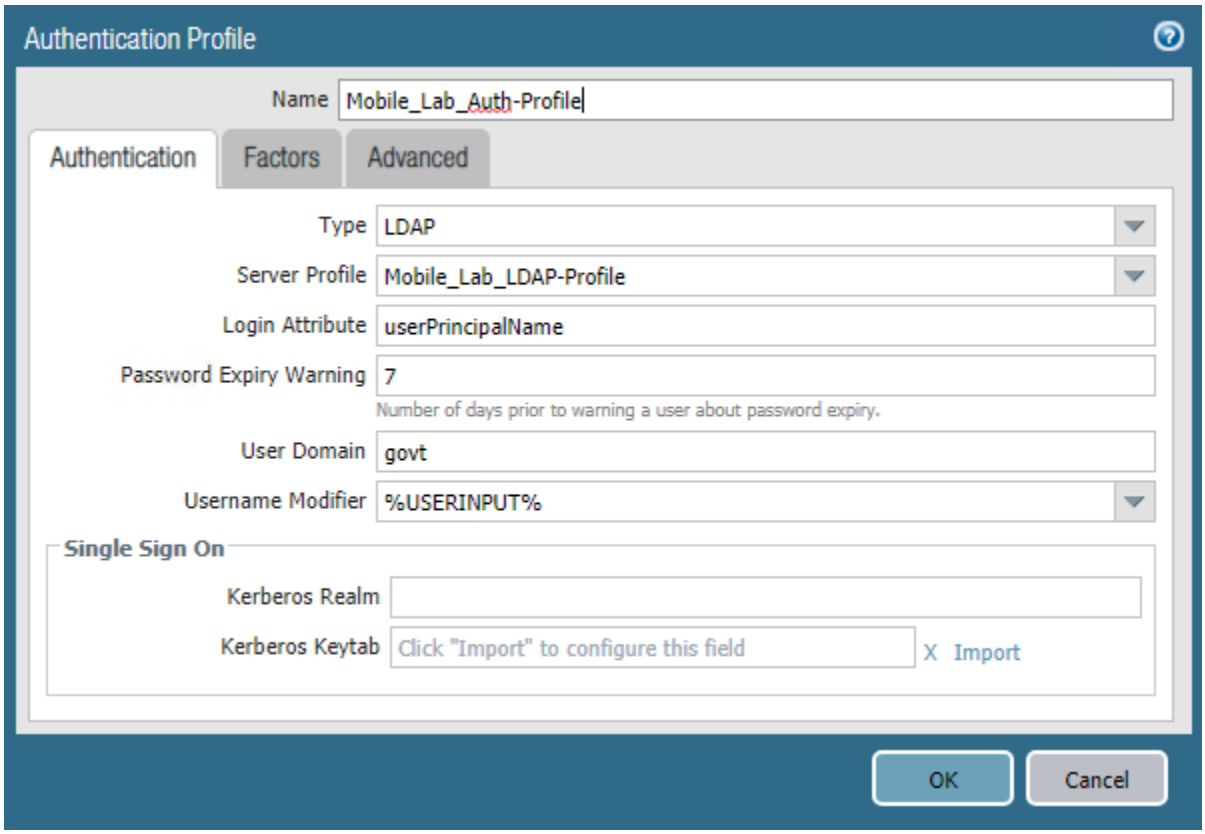


Rysunek 2-56 Profil LDAP

2.5.8.1.2. KONFIGURACJA PROFILU UWIERZYTELNIANIA

1. W portalu **Palo Alto Networks** wybierz kolejno opcje **Device** (Urządzenie) > **Authentication Profile** (Profil uwierzytelniania).
2. Poniżej okienka szczegółów kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **Authentication Profile** (Profil uwierzytelniania).
3. W formularzu **Authentication Profile** (Profil uwierzytelniania):
    a. W polu **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi identyfikację tego profilu uwierzytelniania.
    b. Na karcie **Authentication** (Uwierzytelnianie):
        i. Z menu rozwijanego **Type** (Typ) wybierz opcję **LDAP**.
        ii. Z menu rozwijanego **Server Profile** (Profil serwera) wybierz nazwę profilu serwera LDAP utworzonego w poprzednim punkcie.
        iii. W polu **Login Attribute** (Atrybut logowania) wpisz **userPrincipalName**.

iv. W polu **User Domain** (Domena użytkownika) wprowadź nazwę domeny przedsiębiorstwa. W naszym przykładowym wdrożeniu użyto domeny **govt**.



Rysunek 2-57 Profil uwierzytelniania

c. Wybierz kartę **Advanced** (Zaawansowane).

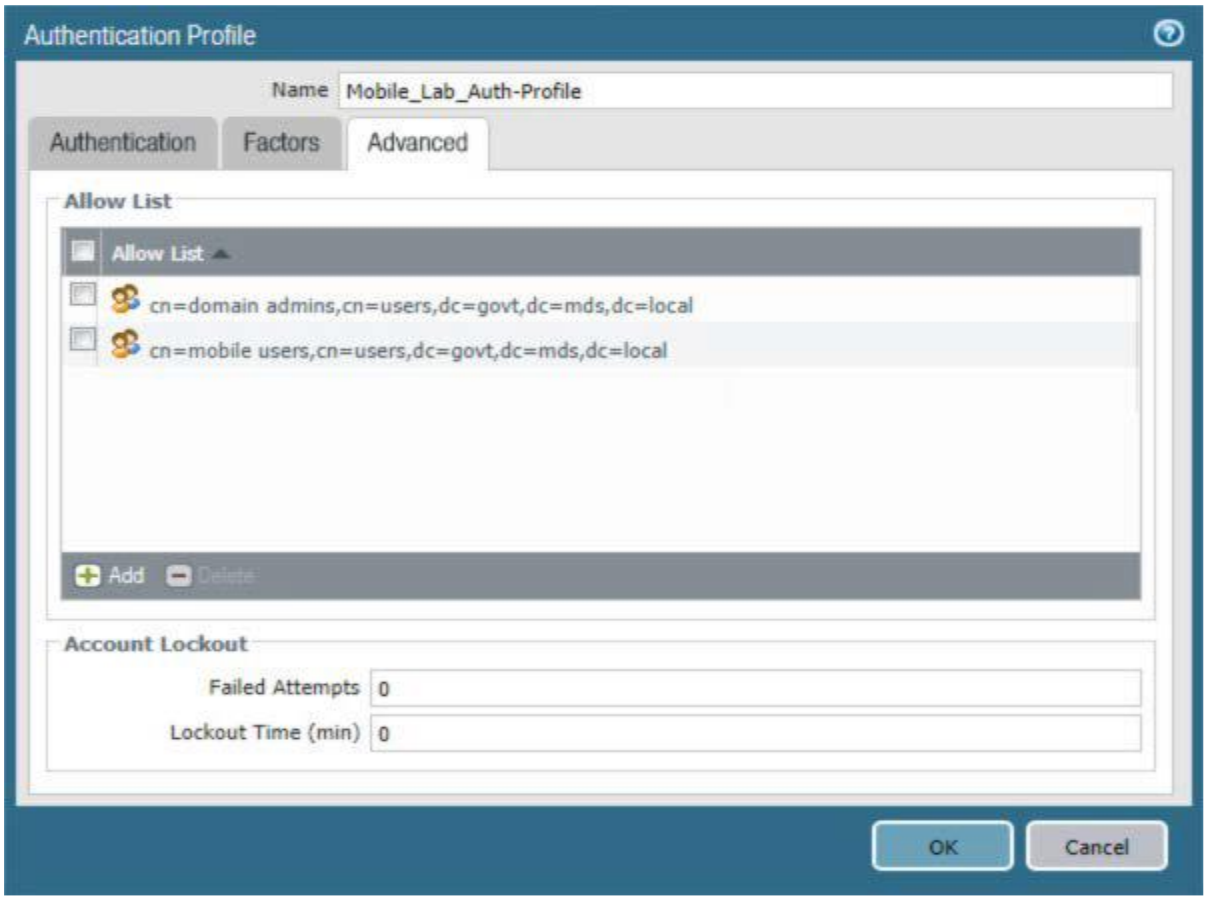
d. Na karcie **Advanced** (Zaawansowane):

i. Pod polem **Allow List** (Lista dozwolonych) kliknij przycisk **Add** (Dodaj). Na liście zostanie utworzona nowa pozycja.

ii. W nowej pozycji na liście wybierz grupę Active Directory dla użytkowników mobilnych.

iii. Powtórz kroki 3di i 3dii dla wszystkich dodatkowych grup, które powinny uwierzytelniać się w sieci SSL VPN.

e. Kliknij przycisk **OK**.



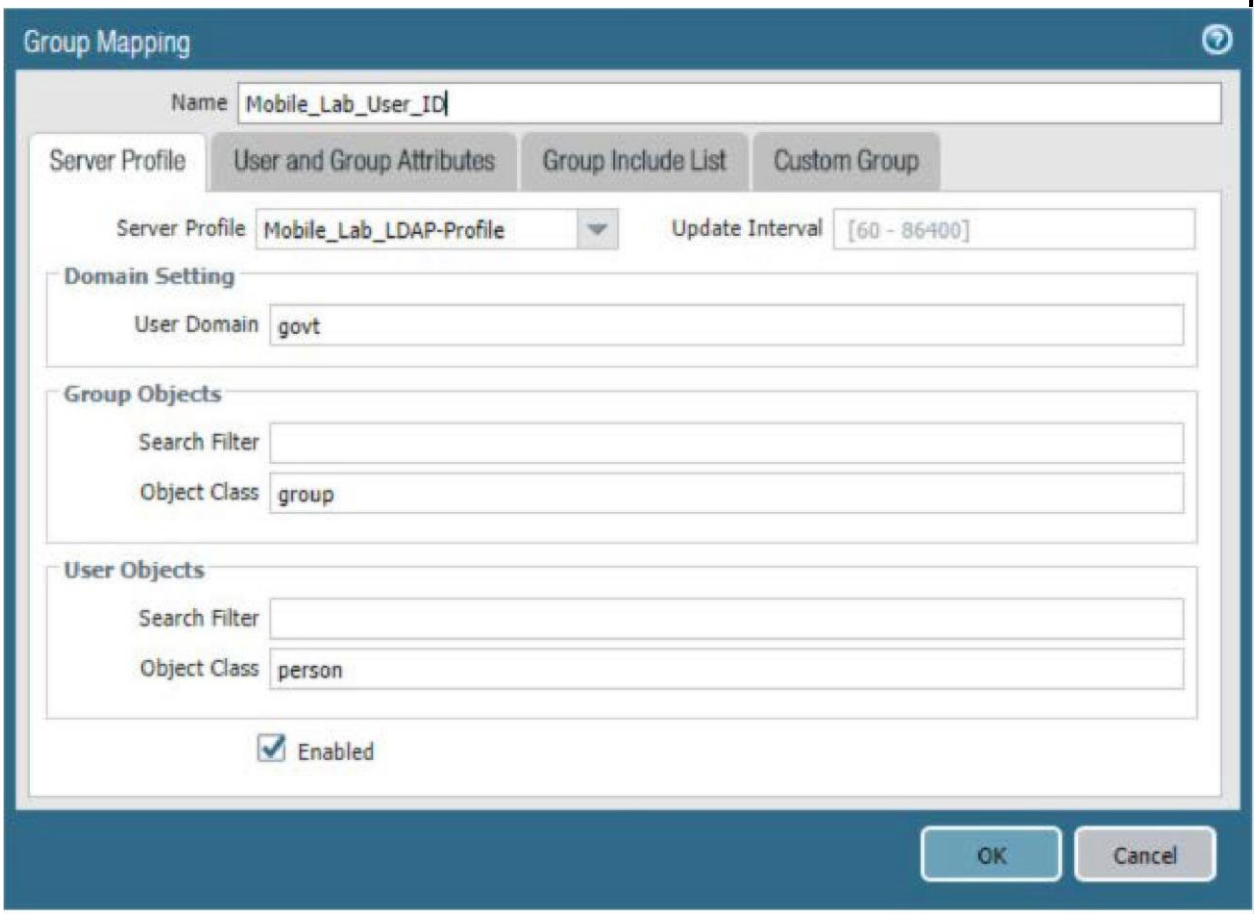
Rysunek 2-58 Zaawansowane ustawienia profilu uwierzytelniania

2.5.8.1.3. KONFIGURACJA IDENTYFIKACJI UŻYTKOWNIKA

1. W portalu **Palo Alto Networks** przejdź do obszaru **Device & User Identification** (Identyfikacja urządzeń i użytkowników).
2. W okienku szczegółów wybierz kartę **Group Mapping Settings** (Ustawienia mapowania grupy).
3. Poniżej okienka szczegółów kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **Group Mapping** (Mapowanie grupy).
4. W formularzu **Group Mapping** (Mapowanie grupy):
    a. W polu **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi identyfikację tego mapowania grupy.
    b. Na karcie **Server Profile** (Profil serwera):

i. Z menu rozwijanego **Server Profile** (Profil serwera) wybierz utworzony wcześniej profil serwera LDAP.

ii. W polu **Domain Setting** (Ustawienia domeny) > **User Domain** (Domena użytkownika) wprowadź nazwę domeny Active Directory. W przykładowym wdrożeniu użyto domeny **govt**.



Rysunek 2-59 Mapowanie grupy LDAP

c. Wybierz kartę **Group Includes List** (Lista dołączonych grup).

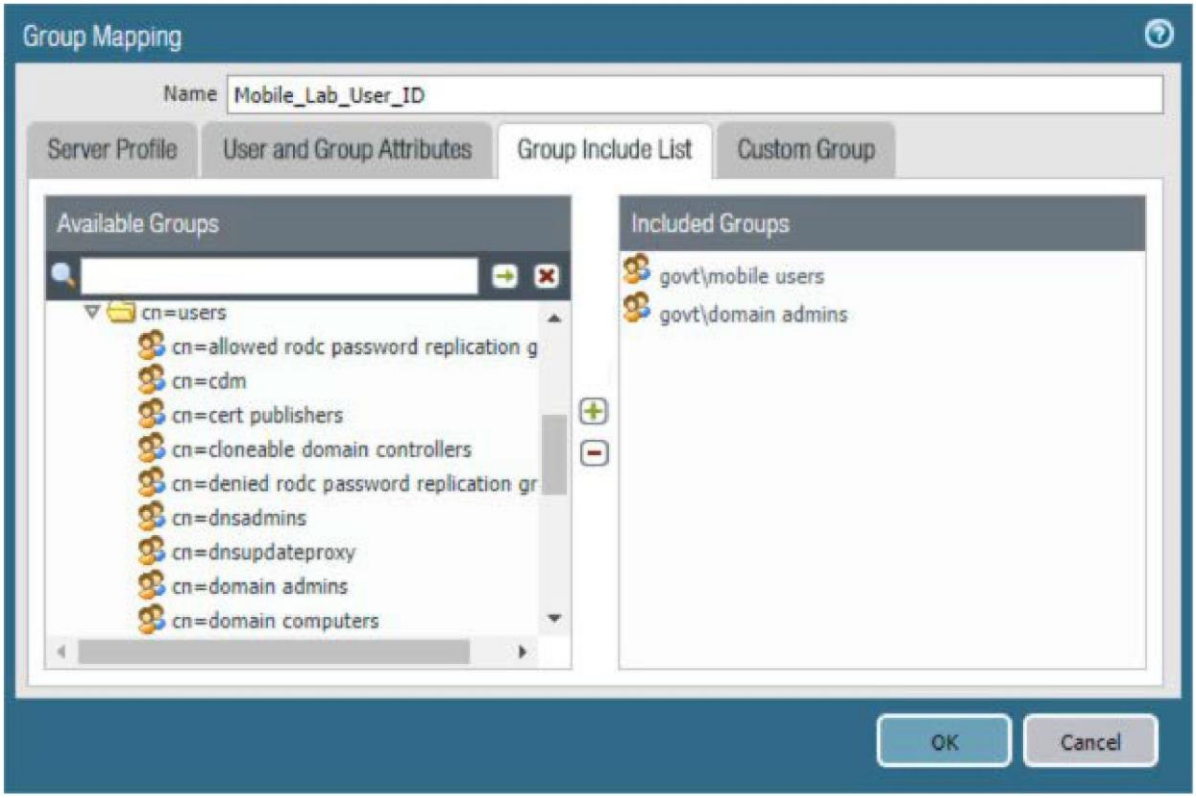
d. Na karcie **Group Includes List** (Lista dołączonych grup):

i. W polu listy **Available Groups** (Dostępne grupy) rozwiń domenę Active Directory, aby wyświetlić skonfigurowane grupy użytkowników.

ii. Dla każdej grupy **Active Directory**, która ma być uwzględniona w tej konfiguracji identyfikacji użytkownika:

1) Wybierz grupę Active Directory.

2) Kliknij ikonę plusa, aby przenieść grupę do listy **Included Groups** (Dołączone grupy).



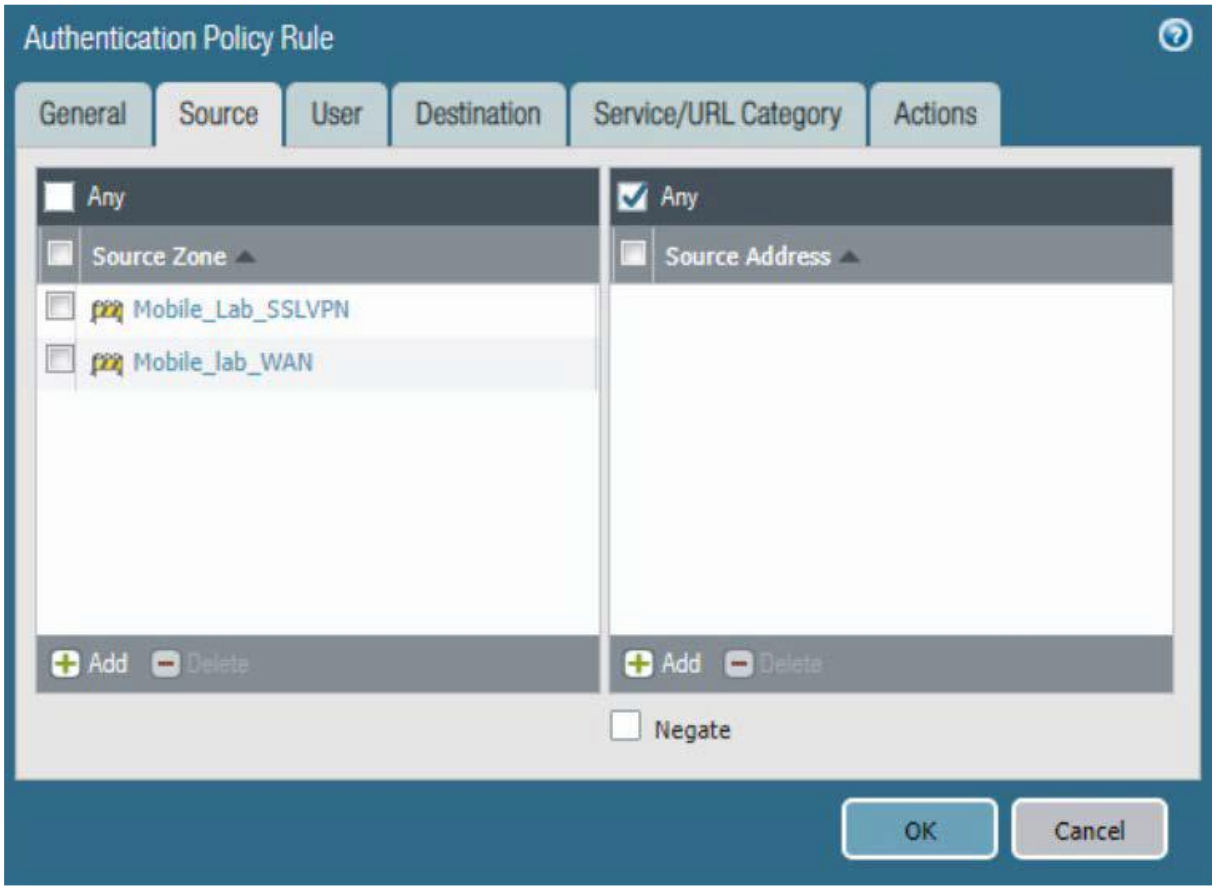
Rysunek 2-60 Lista dołączonych grup LDAP

5. Kliknij przycisk **OK**.

2.5.8.1.4. KONFIGURACJA REGUŁY UWIERZYTELNIANIA

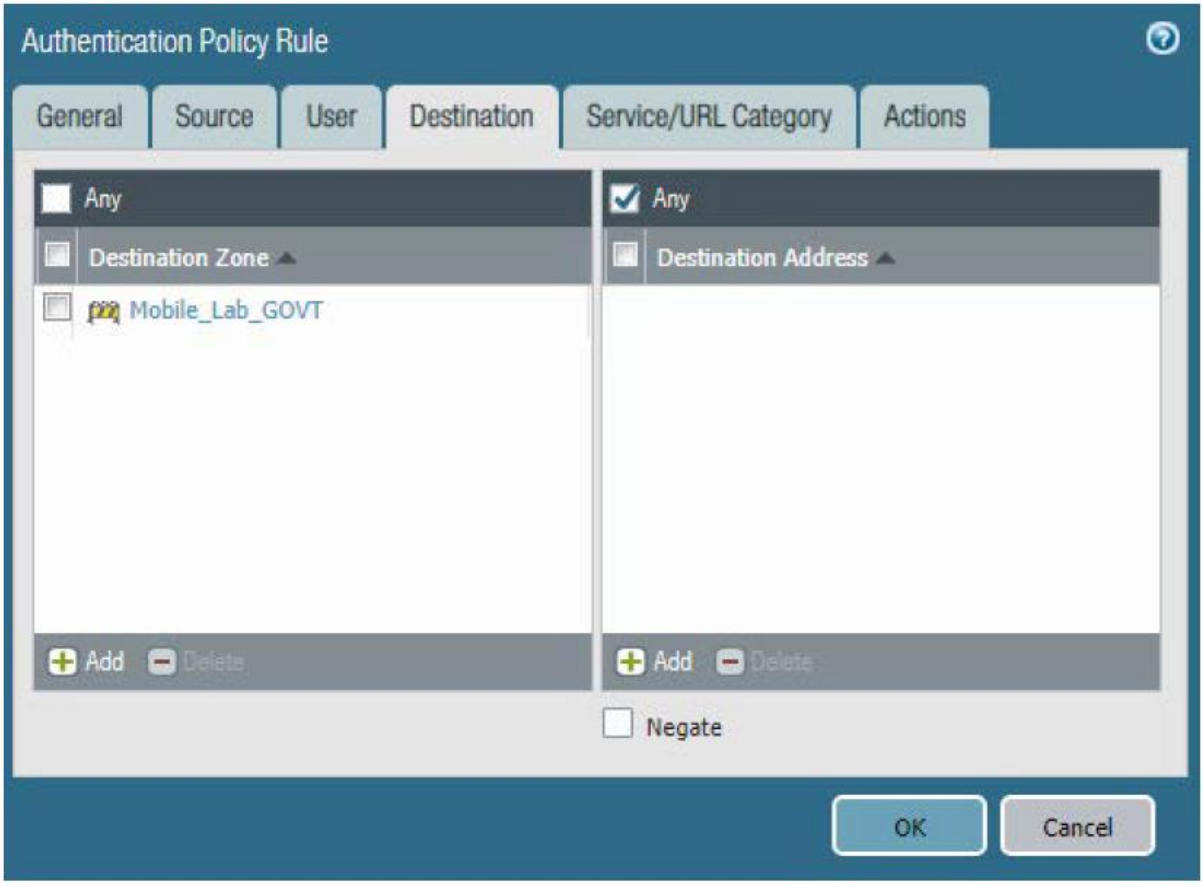
1. Przejdź do obszaru **Policies** (Zasady) > **Authentication** (Uwierzytelnianie).
2. Kliknij przycisk **Add** (Dodaj).
3. Nadaj zasadzie nazwę. W tym wdrożeniu użyto nazwy **Mobile_Lab_Auth_Rule**.
4. Kliknij kartę **Source** (Źródło).

5. Kliknij przycisk **Add** (Dodaj) znajdujący się pod obszarem **Source Zone** (Strefa źródłowa). Wybierz strefę **SSL VPN**.
6. Kliknij przycisk **Add** (Dodaj) znajdujący się pod obszarem **Source Zone** (Strefa źródłowa). Wybierz strefę **WAN**.



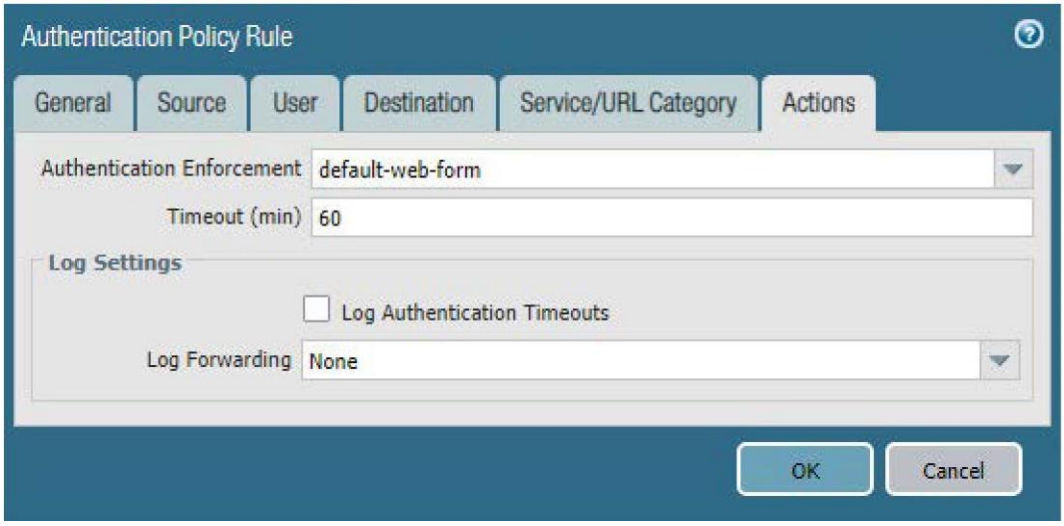
Rysunek 2-61 Strefy źródłowe dla zasady uwierzytelniania

7. Kliknij kartę **Destination** (Lokalizacja docelowa).
8. Kliknij przycisk **Add** (Dodaj) znajdujący się pod obszarem **Destination Zone** (Strefa docelowa).
9. Wybierz strefę **LAN** (w tym wdrożeniu Mobile_Lab_GOVT).



Rysunek 2-62 Strefy docelowe dla zasady uwierzytelniania

10. Kliknij kartę **Service/URL Category** (Kategoria usługi/URL).
11. Kliknij przycisk **Add** (Dodaj) znajdujący się pod obszarem **Service** (Usługa).
12. Wybierz opcję **service-http**.
13. Kliknij przycisk **Add** (Dodaj) znajdujący się obszarem **Service** (Usługa).
14. Wybierz opcję **service-https**.
15. Kliknij kartę **Actions** (Akcje).
16. W polu **Authentication Enforcement** (Wymuszanie uwierzytelniania), wybierz opcję **default-web-form.**
17. W polach **Timeout** (Limit czasu) i **Log Settings** (Ustawienia dziennika) należy pozostawić wartości domyślne.



Rysunek 2-63 Akcje profilu uwierzytelniania

18. Kliknij przycisk **OK** i zatwierdź zmiany.

2.5.9. IMPORTOWANIE CERTYFIKATÓW

Certyfikaty muszą zostać zaimportowane do urządzenia, aby skonfigurować profile certyfikatów, które wpłyną na sposób ich wykorzystania do obsługi komunikacji z innymi systemami. W szczególności certyfikaty urządzeń wydawane urządzeniom mobilnym będą wykorzystywane do identyfikacji i uwierzytelniania użytkowników mobilnych.

Uwaga: Klucze prywatne certyfikatów muszą być chronione hasłem, aby można je było zaimportować do zapory sieciowej.

1. W portalu **Palo Alto Networks** wybierz kolejno opcje **Device** (Urządzenie) > **Certificate Management** (Zarządzanie certyfikatami) > **Certificates** (Certyfikaty).
2. Poniżej okienka szczegółów kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **Import Certificate** (Importuj certyfikat).
3. W formularzu **Import Certificate** (Importuj certyfikat):
    a. Dla ustawienia **Certificate Type** (Typ certyfikatu) zaznacz opcję **Local** (Lokalny).
    b. W polu **Certificate Name** (Nazwa certyfikatu) wprowadź unikalną nazwę, która umożliwi identyfikację tego certyfikatu.

c. Obok pola **Certificate File** (Plik certyfikatu) wybierz opcję **Browse...** (Przeglądaj...), aby określić pełną ścieżkę do pliku zawierającego certyfikat.

d. Z menu rozwijanego **File Format** (Format pliku) wybierz kodowanie certyfikatu odpowiednie dla pliku certyfikatu. W tym przykładzie założono, że certyfikat i klucz prywatny znajdują się w osobnych plikach, i wybrano opcję **PEM**. Uwaga: Klucz prywatny certyfikatu musi być chroniony hasłem, aby można go było zaimportować do urządzeń Palo Alto Networks.

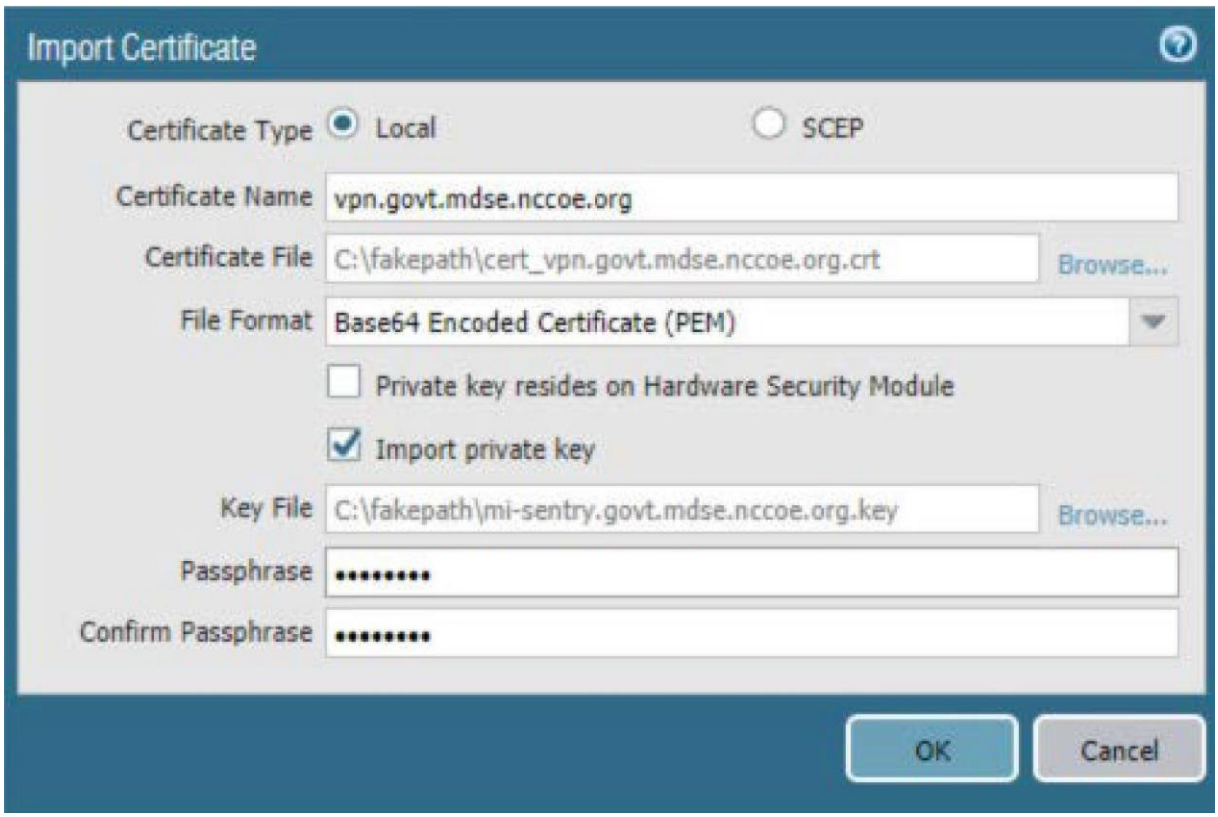
e. Jeśli certyfikat służy do identyfikacji urządzenia Palo Alto Networks:

    i. Zaznacz pole wyboru **Import private key** (Importuj klucz prywatny).

    ii. Obok pola **Key File** (Plik klucza) wybierz opcję **Browse...** (Przeglądaj...), aby określić pełną ścieżkę do pliku zawierającego klucz prywatny dla przesłanego certyfikatu.

    iii. W polu **Passphrase** (Hasło) wprowadź hasło chroniące klucz prywatny.

    iv. W polu **Confirm Passphrase** (Potwierdź hasło) ponownie wprowadź hasło chroniące klucz prywatny.



Rysunek 2-64 Importowanie certyfikatu MobileIron

f. Kliknij przycisk **OK**.

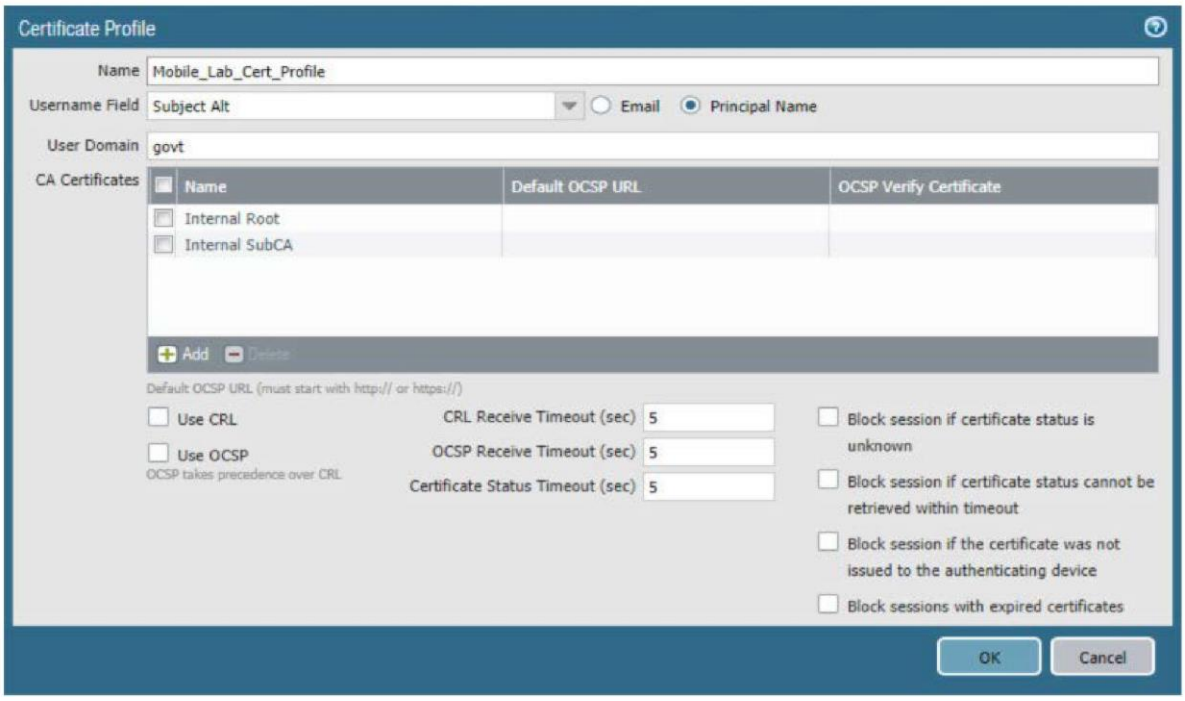
4. Powtórz krok 3 dla każdego certyfikatu, który ma zostać zaimportowany do urządzenia Palo Alto Networks. Dotyczy to wszystkich certyfikatów, których urządzenie będzie używać do identyfikowania się lub uwierzytelniania w systemach zdalnych, wszystkich certyfikatów w łańcuchu zaufania dla każdego takiego certyfikatu oraz wszelkich certyfikatów łańcucha zaufania obsługujących weryfikację tożsamości dla systemów zdalnych, w których to urządzenie będzie wymagać identyfikacji i uwierzytelniania opartego na certyfikatach. W tym przykładowym wdrożeniu certyfikaty są wykorzystywane dla następujących systemów:

- certyfikat serwera dla tego urządzenia wydany przez DigiCert
- certyfikat głównego CA DigiCert
- certyfikat podrzędnego CA DigiCert

- główny certyfikat przedsiębiorstwa Microsoft CA
- certyfikat podrzędnego CA przedsiębiorstwa Microsoft CA

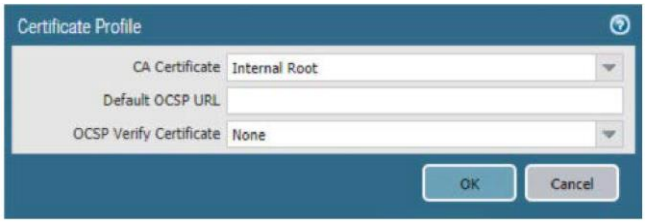
2.5.10. KONFIGUROWANIE PROFILU CERTYFIKATU

1. W portalu **Palo Alto Networks** wybierz kolejno opcje **Certificate Management** (Zarządzanie certyfikatami) > **Certificate Profile** (Profil certyfikatu).
2. Poniżej okienka szczegółów kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **Certificate Profile** (Profil certyfikatu).
3. W formularzu **Certificate Profile** (Profil certyfikatu):
   a. W polu **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi identyfikację tego profilu certyfikatu.
   b. W menu rozwijanym **Username Field** (Pole nazwy użytkownika) wybierz opcję **Subject Alt** (Alternatywna nazwa podmiotu).
   c. Zaznacz opcję **Principal Name** (Nazwa główna).
   d. W polu **User Domain** (Domena użytkownika) wprowadź nazwę domeny Active Directory dla swojego przedsiębiorstwa. W tym przykładowym wdrożeniu użyto domeny **govt**.
   e. Pod polem listy **CA Certificate** (Certyfikat CA) kliknij przycisk **Add** (Dodaj). Pojawi się dodatkowy formularz **Certificate Profile** (Profil certyfikatu).
   f. W dodatkowym formularzu **Certificate Profile** (Profil certyfikatu) z rozwijanego menu **CA Certificate** (Certyfikat CA) wybierz certyfikat główny Microsoft Active Directory Certificate Services przesłany w ramach wykonywania **punktu 2.5.9**.
   g. Kliknij przycisk **OK**.
   h. Powtórz krok 3f dla każdego certyfikatu pośredniego w łańcuchu zaufania między certyfikatem głównym a certyfikatem podrzędnego urzędu certyfikacji, który wydaje certyfikaty urządzeniom mobilnym.



Rysunek 2-65 Profil certyfikatu

i. Kliknij przycisk **OK**.



Rysunek 2-66 Profil głównego certyfikatu wewnętrznego

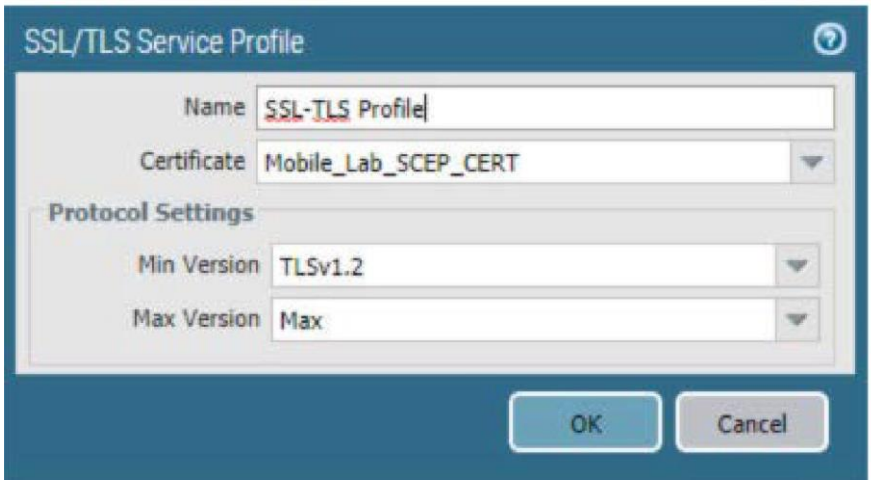
4. Kliknij przycisk OK.

2.5.11. KONFIGUROWANIE PROFILU USŁUGI SSL/TLS

Poniższe kroki umożliwią konfigurowanie profilu SSL/TLS, który określa, jakim certyfikatom należy ufać, gdy urządzenia mobilne łączą się z siecią VPN i jakiego certyfikatu należy używać podczas nawiązywania wychodzących połączeń SSL/TLS.

1. W portalu **Palo Alto Networks** wybierz kolejno opcje **Device** (Urządzenie) > **Certificate Management** (Zarządzanie certyfikatami) > **SSL/TLS Service Profile** (Profil usługi SSL/TLS).

2. Poniżej okienka szczegółów kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **SSL/TLS Service Profile** (Profil usługi SSL/TLS).
3. W formularzu **SSL/TLS Service Profile** (Profil usługi SSL/TLS):
   a. W polu **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi identyfikację tego profilu usługi.
   b. Z menu rozwijanego **Certificate** (Certyfikat) wybierz certyfikat, który ma być używany dla tego profilu usługi SSL/TLS. W naszym przykładowym wdrożeniu używany jest certyfikat klienta uzyskany od ośrodka certyfikacji Microsoft Enterprise za pośrednictwem protokołu SCEP.
   c. Z menu rozwijanego **Min Version** (Wersja min.) wybierz opcję **TLSv1.2.** Z menu **Max Version**, wybierz opcję **Max** (Maks.).
   d. Kliknij przycisk **OK**.



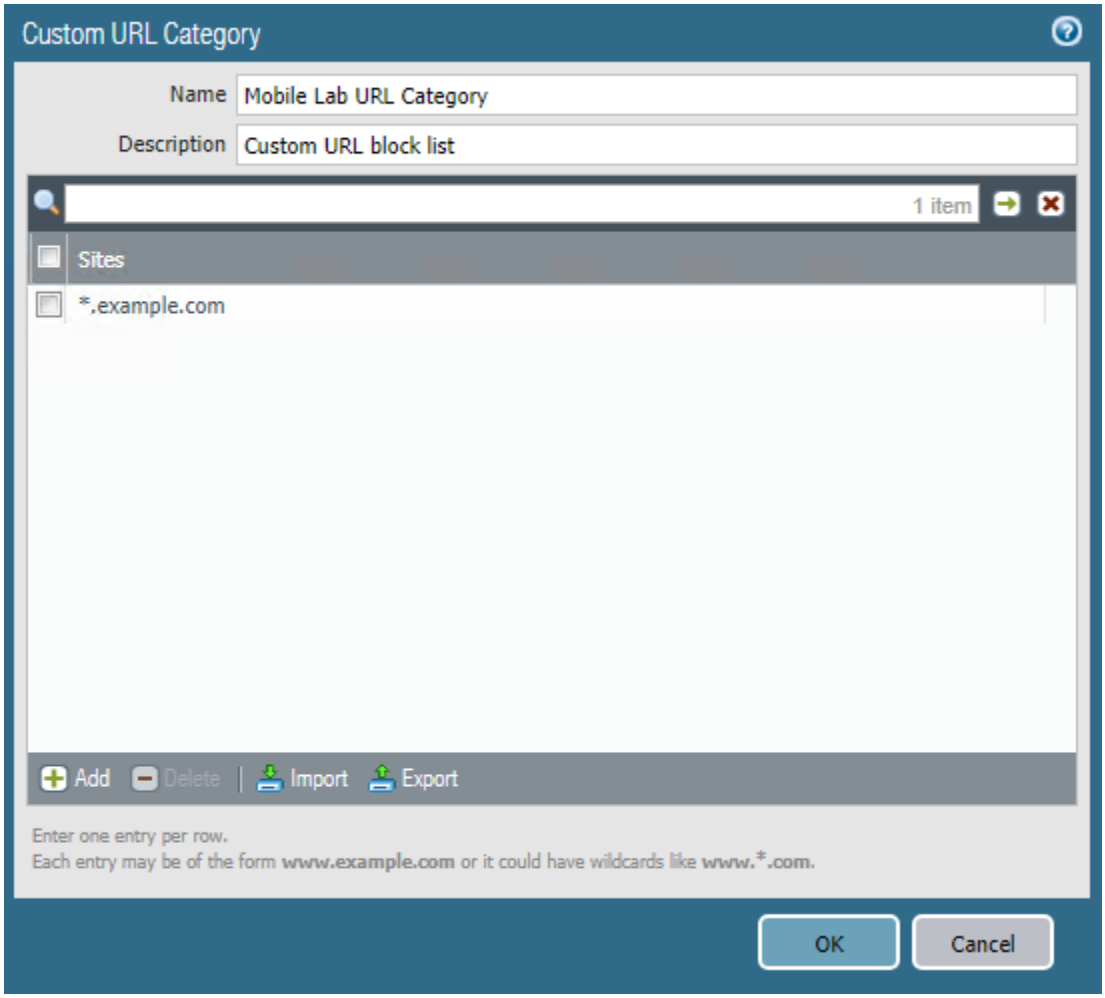
Rysunek 2-67 Profil usługi SSL/TLS

4. Powtórz krok 3, aby dodać identyczny profil usługi SSL/TLS dla certyfikatu serwera tego urządzenia wydanego przez DigiCert.

2.5.12. KONFIGUROWANIE FILTROWANIA ADRESÓW URL

1. Wybierz kolejno opcje **Objects** (Obiekty) > **Custom Objects** (Obiekty niestandardowe) > **URL Category** (Kategorie adresów URL).

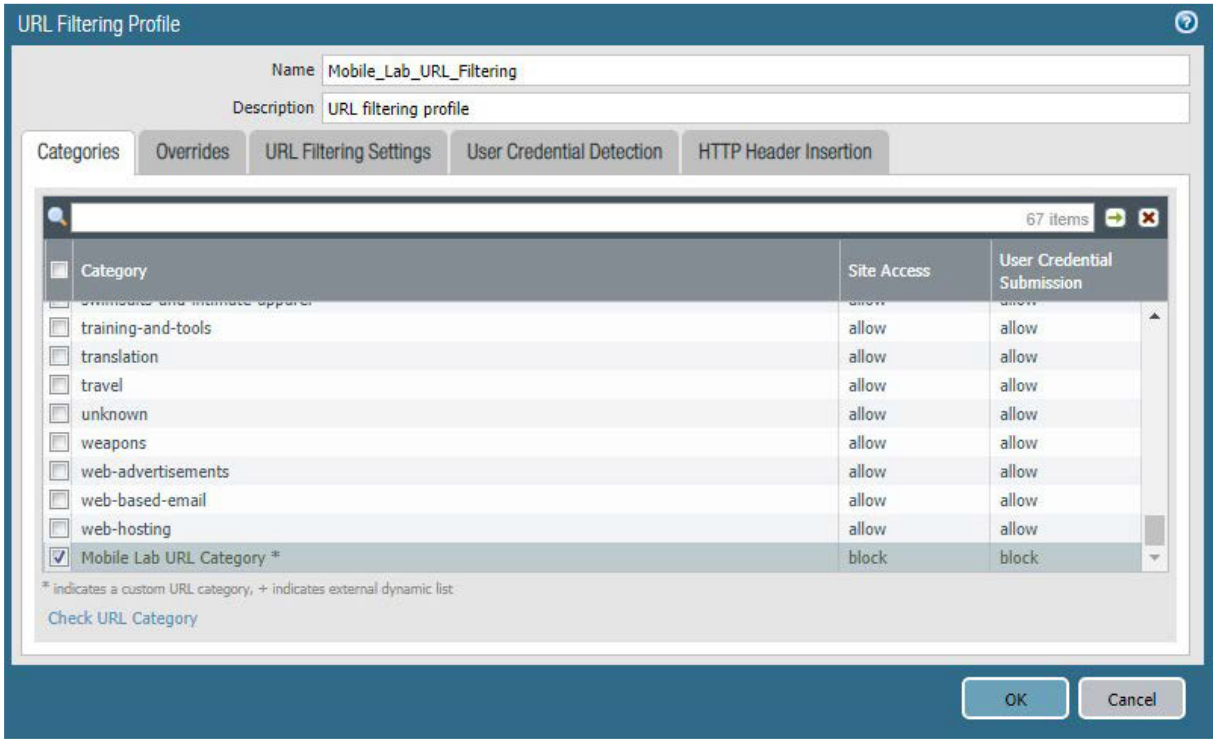
2. Kliknij przycisk **Add** (Dodaj).
3. Nadaj kategorii nazwę i opis.
4. Za pomocą przycisku **Add** (Dodaj) dodaj witryny, które mają być blokowane. W tym przykładzie użyto strony ***.example.com**.



Rysunek 2-68 Niestandardowa kategoria adresów URL

5. Kliknij przycisk OK.
6. Wybierz kolejno opcje **Objects** (Obiekty) > **Security Profiles** (Profile bezpieczeństwa) > **URL Filtering** (Filtrowanie adresów URL).
7. Zaznacz pole obok pozycji domyślnej i kliknij przycisk **Clone** (Klonuj).
8. W wyświetlonym oknie wybierz opcję **default** (domyślny).

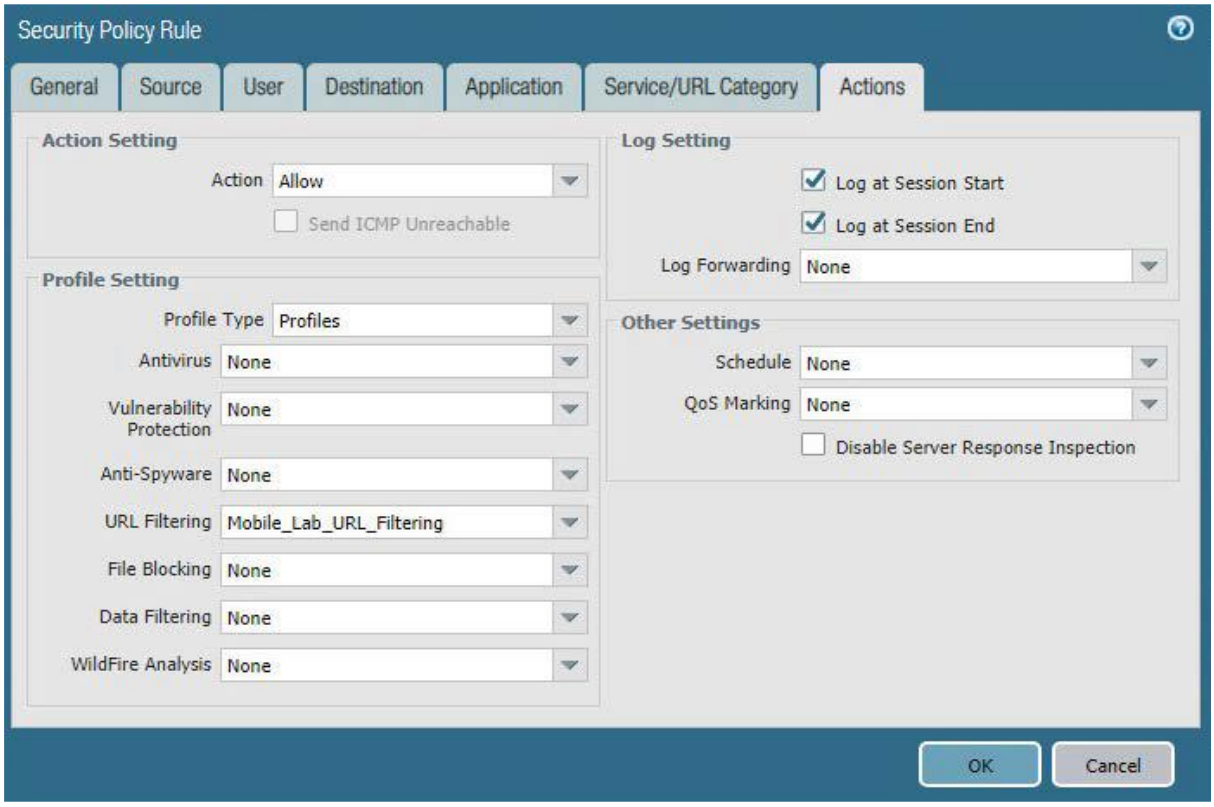
9. Kliknij przycisk **OK**.
10. Kliknij nowo utworzony profil, **default-1**.
11. Nadaj nowo utworzonemu profilowi o nazwie **default-1** odpowiednią nazwę i wprowadź jego opis.
12. Przewiń widok do dołu listy. Nazwa utworzonej kategorii będzie ostatnia na liście.
13. Kliknij opcję w kolumnie **Site Access** (Dostęp do witryny) obok utworzonej kategorii adresów URL.
14. Ustaw opcję **Site Access** (Dostęp do witryny) na **block** (blokuj).



Rysunek 2-69 Profil filtrowania adresów URL

15. Kliknij przycisk **OK**.
16. Przejdź do części **Policies** (Zasady) > **Security** (Bezpieczeństwo).
17. Kliknij domyślną zasadę połączeń wychodzących dla sieci wewnętrznej (nie VPN).

18. Kliknij kartę **Actions** (Akcje).
19. W polu **Profile Type** (Typ profilu) wybierz opcję **Profiles** (Profile).
20. W polu **URL Filtering** (Filtrowanie adresów URL) wybierz nowo utworzony profil.
21. Kliknij przycisk **OK**.
22. Powtórz kroki od 18 do 21 dla ruchu wychodzącego SSL VPN.



Rysunek 2-70 Zasady bezpieczeństwa filtrowania adresów URL

23. W prawym górnym rogu kliknij przycisk **Commit** (Zatwierdź).
24. W oknie podręcznym kliknij przycisk **Commit** (Zatwierdź).

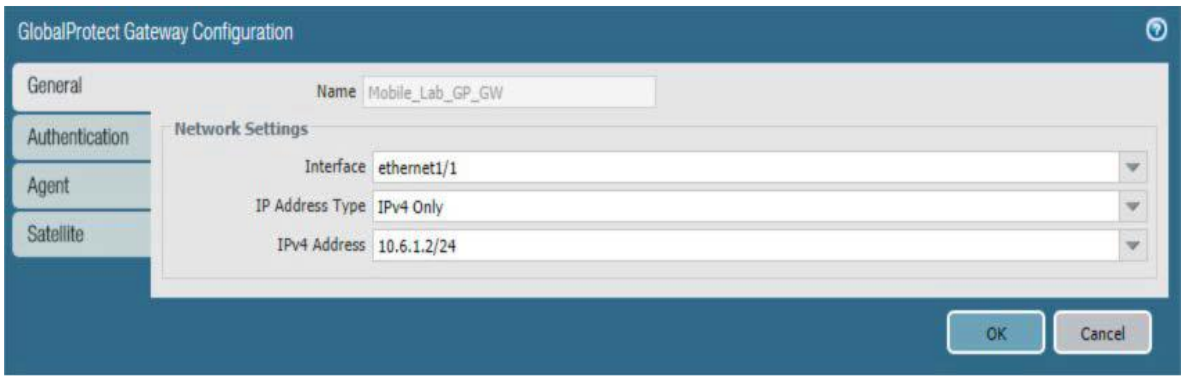
2.5.13. KONFIGUROWANIE BRAMY I PORTALU GLOBALPROTECT

Konfiguracja sieci SSL VPN wymaga utworzenia zarówno bramy GlobalProtect, jak i portalu GlobalProtect, który może być używany do zarządzania połączeniami VPN między wieloma bramami. W tym przykładowym wdrożeniu skonfigurowano tylko jedną bramę i portal.

2.5.13.1. KONFIGUROWANIE BRAMY GLOBALPROTECT

Brama GlobalProtect zapewnia użytkownikom zdalnym bezpieczny dostęp do zasobów wewnętrznych w oparciu o ich grupę Microsoft AD. Aby skonfigurować bramę GlobalProtect:

1. W portalu **Palo Alto Networks** wybierz kolejno opcje **Network** (Sieć) > **GlobalProtect** > **Gateways** (Bramy).
2. Poniżej okienka szczegółów kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **GlobalProtect Gateway Configuration** (Konfiguracja bramy GlobalProtect).
3. W formularzu **GlobalProtect Gateway Configuration** (Konfiguracja bramy GlobalProtect), na karcie **General** (Ogólne):
    a. W polu **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi identyfikację tej **bramy GlobalProtect**.
    b. W obszarze **Network Settings** (Ustawienia sieci):
        i. Z menu rozwijanego **Interface** (Interfejs) wybierz interfejs fizyczny podłączony do podsieci, w której znajduje się urządzenie bramy internetowej.
        ii. W menu rozwijanym **IPv4 Address** (Adres IPv4) wybierz adres IP powiązany z interfejsem fizycznym określonym w poprzednim kroku.



Rysunek 2-71 Ogólna konfiguracja bramy GlobalProtect

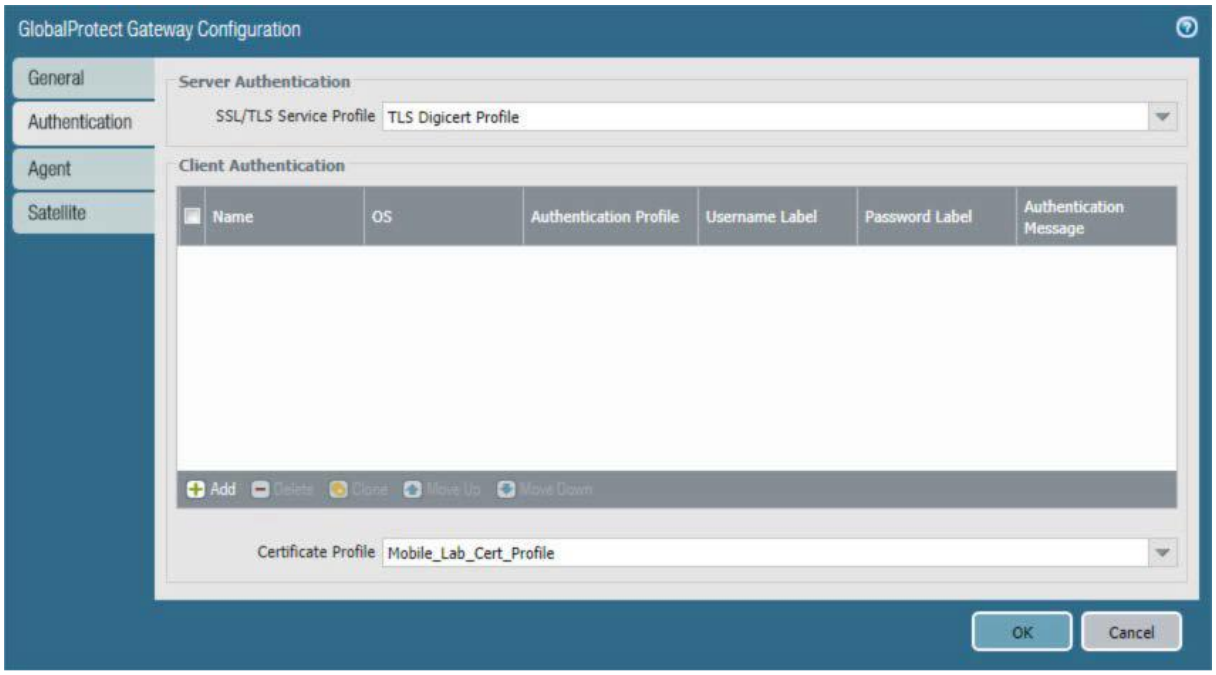
Tłumaczenie

c. Wybierz kartę **Authentication** (Uwierzytelnianie).

d. Na karcie **Authentication** (Uwierzytelnianie):

   i. Z menu rozwijanego **Server Authentication** (Uwierzytelnianie serwera) > **SSL/TLS Service Profile** (Profil usługi SSL/TLS) wybierz profil TLS/SSL powiązany z publicznie zaufanym certyfikatem serwera dla tego urządzenia.

   ii. Z menu rozwijanego **Client Authentication** (Uwierzytelnianie klienta) > **Certificate Profile** (Profil certyfikatu) wybierz profil TLS/SSL klienta powiązany z wewnętrznie zaufanymi certyfikatami klienta wydanymi dla urządzeń mobilnych.



Rysunek 2-72 Konfiguracja uwierzytelniania dla bramy GlobalProtect

e. Wybierz kartę **Agent**.

f. Na karcie **Agent** > **Tunnel Settings** (Ustawienia tunelu):

   i. Zaznacz pole wyboru **Tunnel Mode** (Tryb tunelowy).

   ii. Zaznacz pole wyboru **Enable IPSec** (Włącz IPSec), aby wyłączyć protokół IPSec.

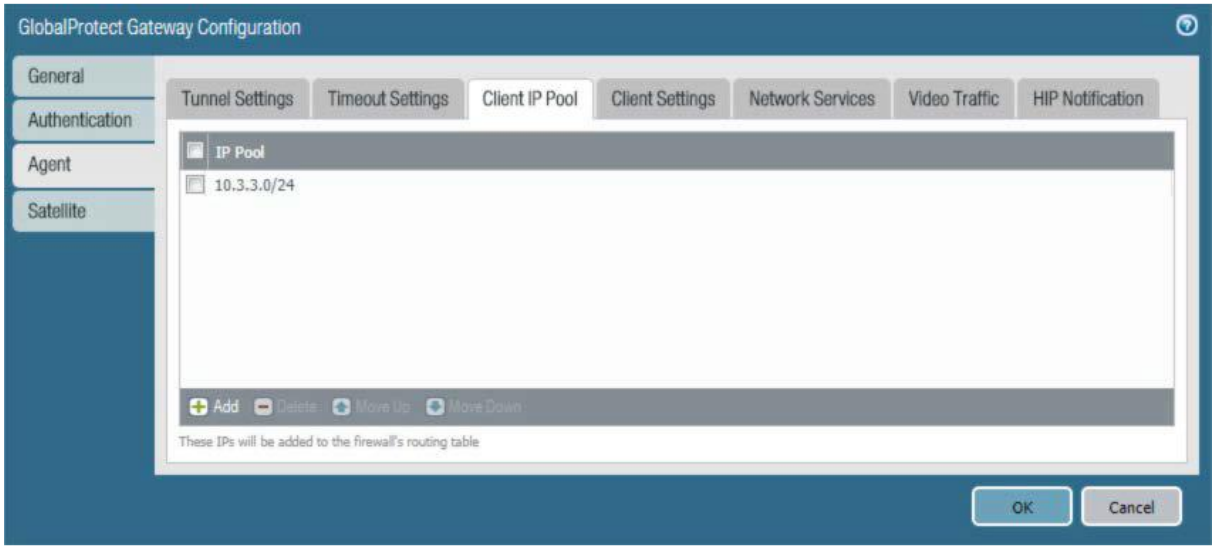
Rysunek 2-73 Konfiguracja tunelu dla bramy GlobalProtect

g. Wybierz kartę **Agent** > **Client IP Pool** (Pula adresów IP klienta).

h. Na karcie **Agent > Client IP Pool** (Pula adresów IP klienta):

   i. Pod polem listy **IP Pool** (Pula adresów IP) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.

   ii. Dla nowej pozycji na liście **IP Pool** (Pula adresów IP) wprowadź adres sieciowy dla puli adresów IP, z której podłączonym urządzeniom zostanie przydzielony adres.

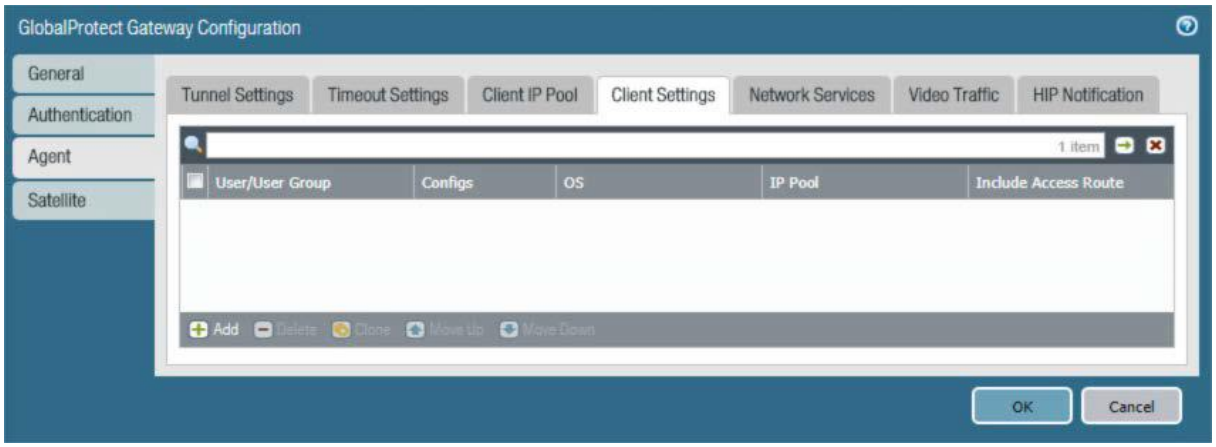


Rysunek 2-74 Pula adresów IP klienta VPN

i. Wybierz kartę **Agent** > **Client Settings** (Ustawienia klienta).

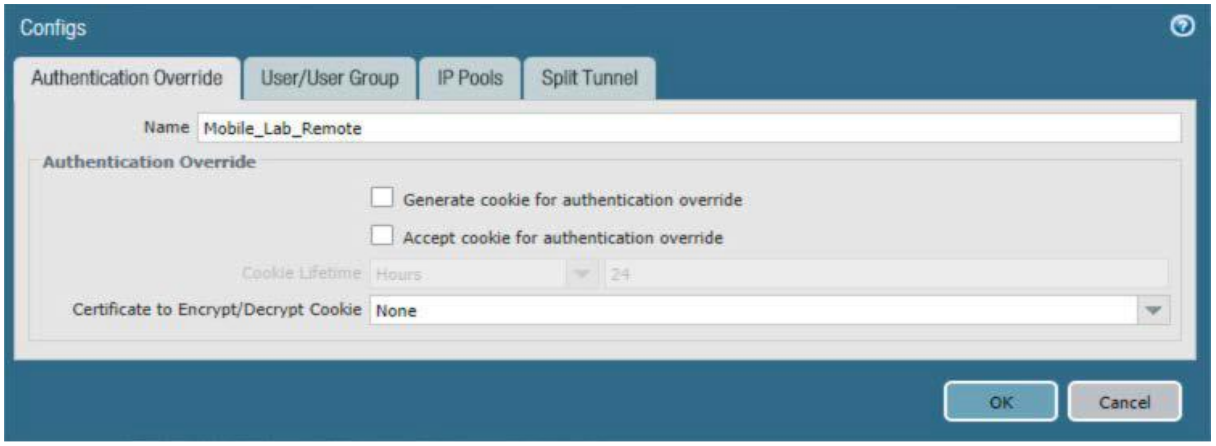
j. Na karcie **Agent** > **Client Settings** (Ustawienia klienta):

   i. Pod polem listy **Client Settings** (Ustawienia klienta) kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **Configs** (Konfiguracje).



Rysunek 2-75 Ustawienia klienta VPN

ii. W formularzu **Configs** (Konfiguracje) na karcie **Authorization Override** (Zastąpienie autoryzacji) wprowadź unikalną nazwę, która umożliwi identyfikację tej konfiguracji klienta.



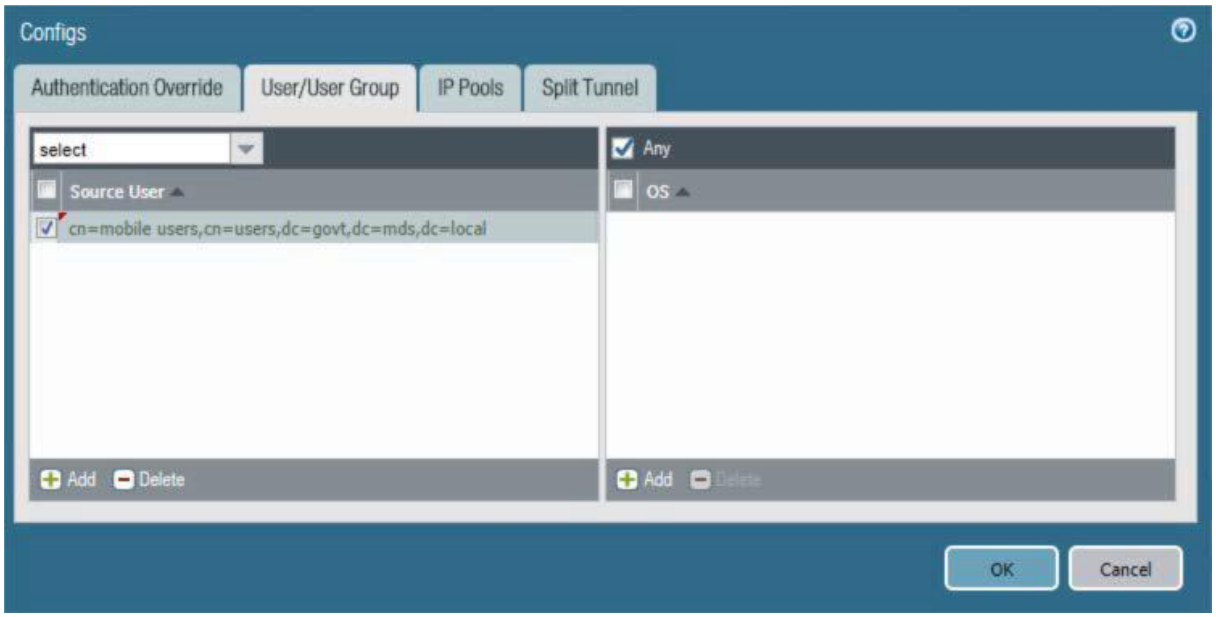
Rysunek 2-76 Konfiguracja zastąpienia uwierzytelniania w sieci VPN

iii. Wybierz kartę **User/User Group** (Użytkownik/grupa użytkowników).

iv. Na karcie **User/User Group** (Użytkownik/grupa użytkowników):

1) Pod polem listy **Source User** (Użytkownik źródłowy) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.

2) W pozycji na liście **Source User** (Użytkownik źródłowy) wybierz grupę użytkowników Microsoft AD, która ma mieć dostęp do zasobów wewnętrznych za pośrednictwem tej bramy GlobalProtect.



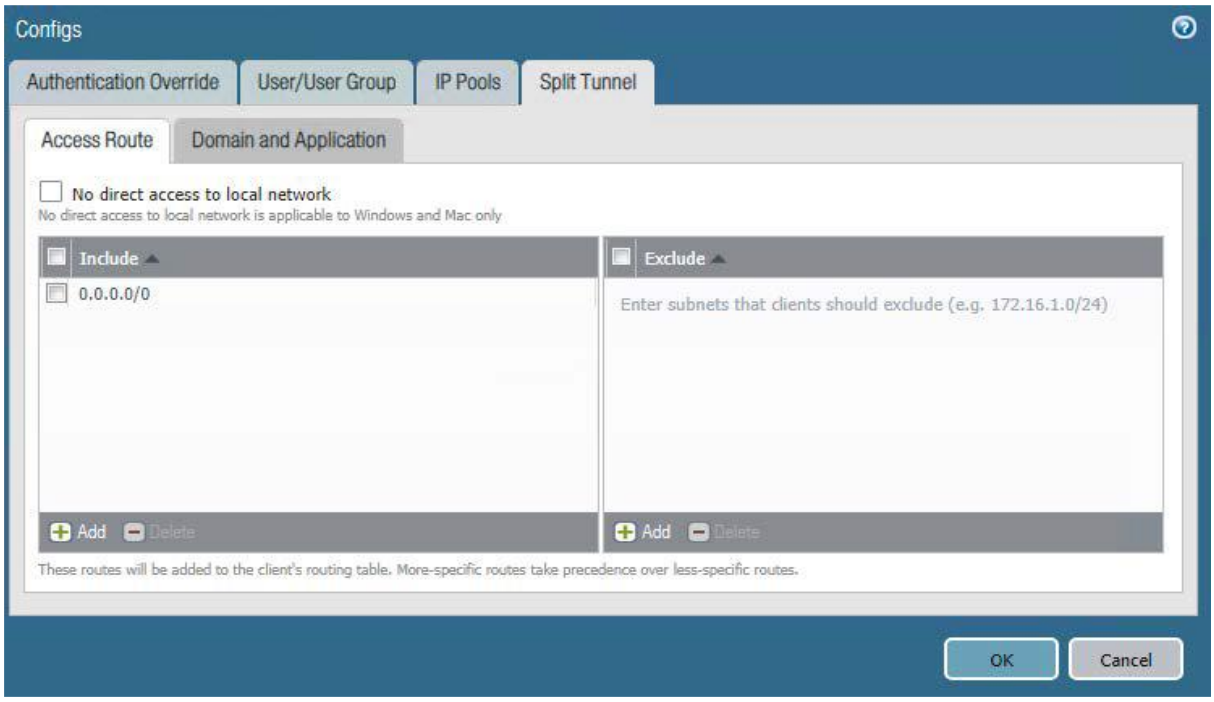
Rysunek 2-77 Konfiguracja grupy użytkowników sieci VPN

v. Wybierz kartę **Split Tunnel** (Tunel dzielony).

vi. Na karcie **Split Tunnel** (Tunel dzielony), w obszarze **Access Route** (Ścieżka dostępu):

1) Pod polem listy **Include** (Dołącz) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.

2) W nowej pozycji na liście **Include** (Dołącz) wprowadź **0.0.0.0/0.** Spowoduje to wymuszenie pełnego tunelowania.



Rysunek 2-78 Konfiguracja tunelu dzielonego dla sieci VPN

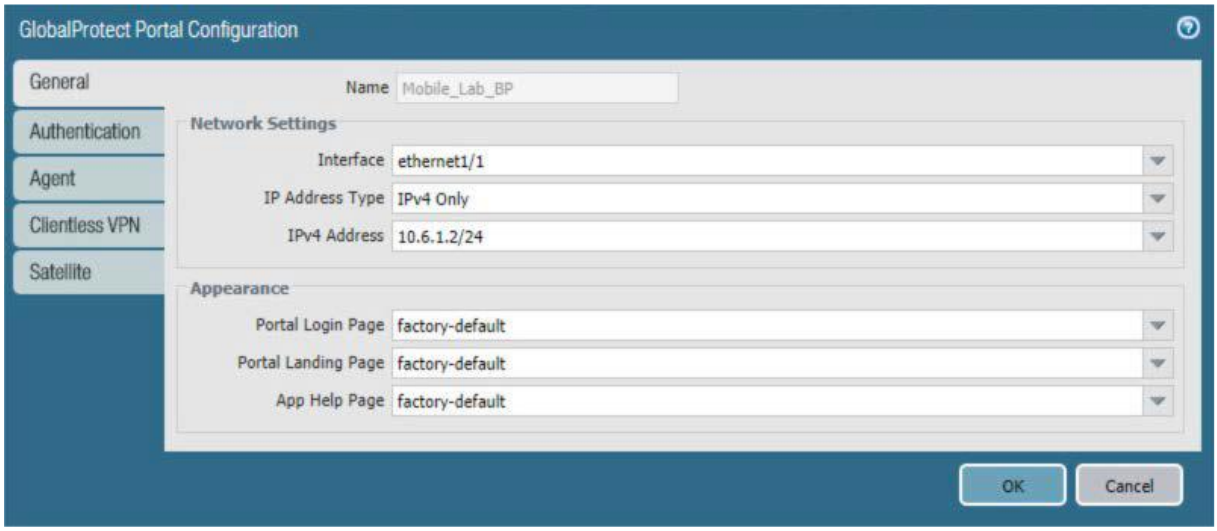
vii. Kliknij przycisk **OK**.

k. Kliknij przycisk **OK**.

2.5.13.2. KONFIGUROWANIE PORTALU GLOBALPROTECT

1. W portalu **Palo Alto Networks** wybierz kolejno opcje **Network** (Sieć) > **GlobalProtect** > **Portal**.
2. Poniżej okienka szczegółów kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **GlobalProtect Portal Configuration** (Konfiguracja portalu GlobalProtect).
3. W formularzu **GlobalProtect Portal Configuration** (Konfiguracja portalu GlobalProtect), na karcie **General** (Ogólne):
   a. W polu **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi identyfikację tego portalu GlobalProtect.
   b. Z menu rozwijanego **Interface** (Interfejs) wybierz interfejs fizyczny podłączony do podsieci, w której znajduje się urządzenie bramy internetowej.

c. Z menu rozwijanego **IP Address Type** (Typ adresu IP) wybierz opcję **IPv4 Only** (Tylko IPv4).



Rysunek 2-79 Konfiguracja portalu GlobalProtect

4. Wybierz kartę **Authentication** (Uwierzytelnianie).

5. Na karcie **Authentication** (Uwierzytelnianie):

   a. Z menu rozwijanego **Server Authentication** (Uwierzytelnianie serwera) > **SSL/TLS Service Profile** (Profil usługi SSL/TLS) wybierz profil usługi SSL/TLS oparty na certyfikacie zewnętrznego serwera.

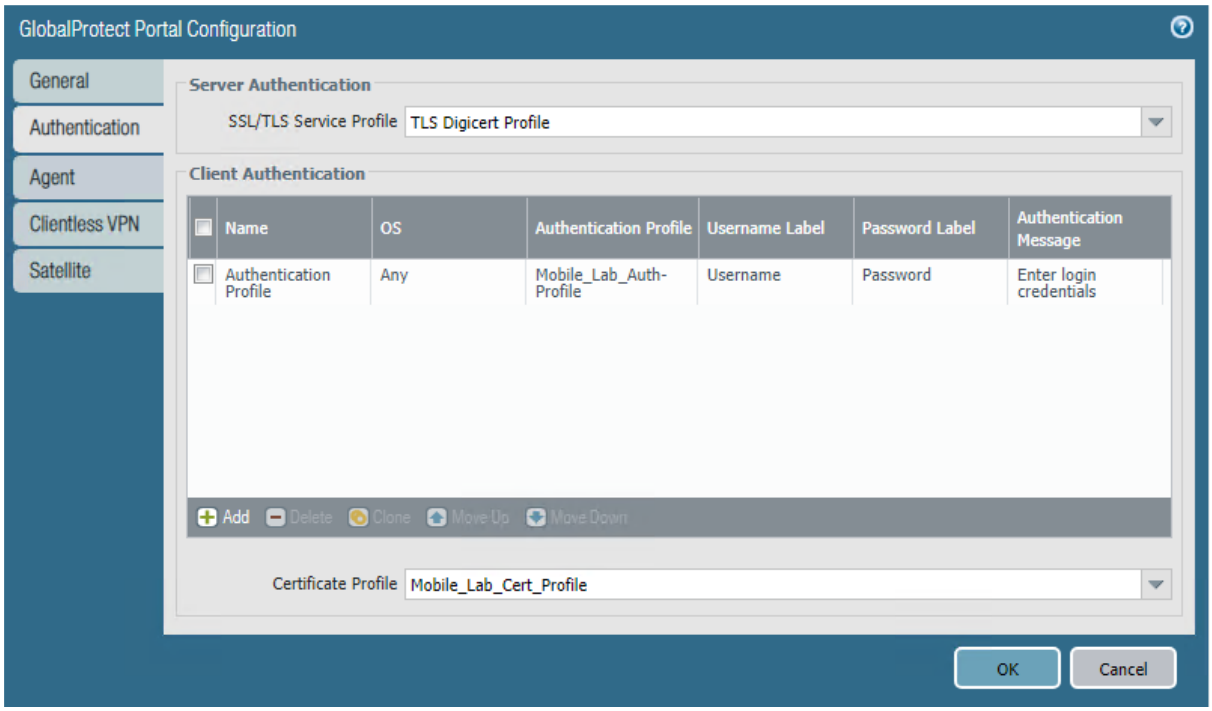
   b. Z menu rozwijanego **Certificate Profile** (Profil certyfikatu) wybierz profil TLS/SSL klienta powiązany z wewnętrznie zaufanymi certyfikatami klienta wydanymi dla urządzeń mobilnych.

   c. Kliknij przycisk **Add** (Dodaj).

   d. Wprowadź nazwę profilu. W tym przykładowym wdrożeniu wykorzystano nazwę **Client Authentication** (Uwierzytelnianie klienta).

   e. Z menu rozwijanego **Authentication Profile** (Profil uwierzytelniania) wybierz utworzony wcześniej profil uwierzytelniania.

   f. Kliknij przycisk **OK**.



Rysunek 2-80 Konfiguracja protokołu SSL/TLS portalu GlobalProtect

6. Wybierz kartę **Agent**.

7. Na karcie **Agent**:

    a. Poniżej pola listy **Agent** kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **Configs** (Konfiguracje).

    b. W formularzu **Configs** (Konfiguracje):

        i. Na karcie **Authentication** (Uwierzytelnianie), w obszarze **Components that Require Dynamic Passwords** (Komponenty wymagające haseł dynamicznych), zaznacz pole wyboru **Portal**.

        ii. Na karcie **External** (Zewnętrzne), pod polem listy **External Gateways** (Zewnętrzne bramy) kliknij przycisk **Add** (Dodaj). Zostanie otwarty formularz **External Gateway** (Brama zewnętrzna).

        iii. W formularzu **External Gateway** (Brama zewnętrzna):

            1) W polu **Name** (Nazwa) wprowadź unikalną nazwę, która umożliwi identyfikację tej bramy zewnętrznej.

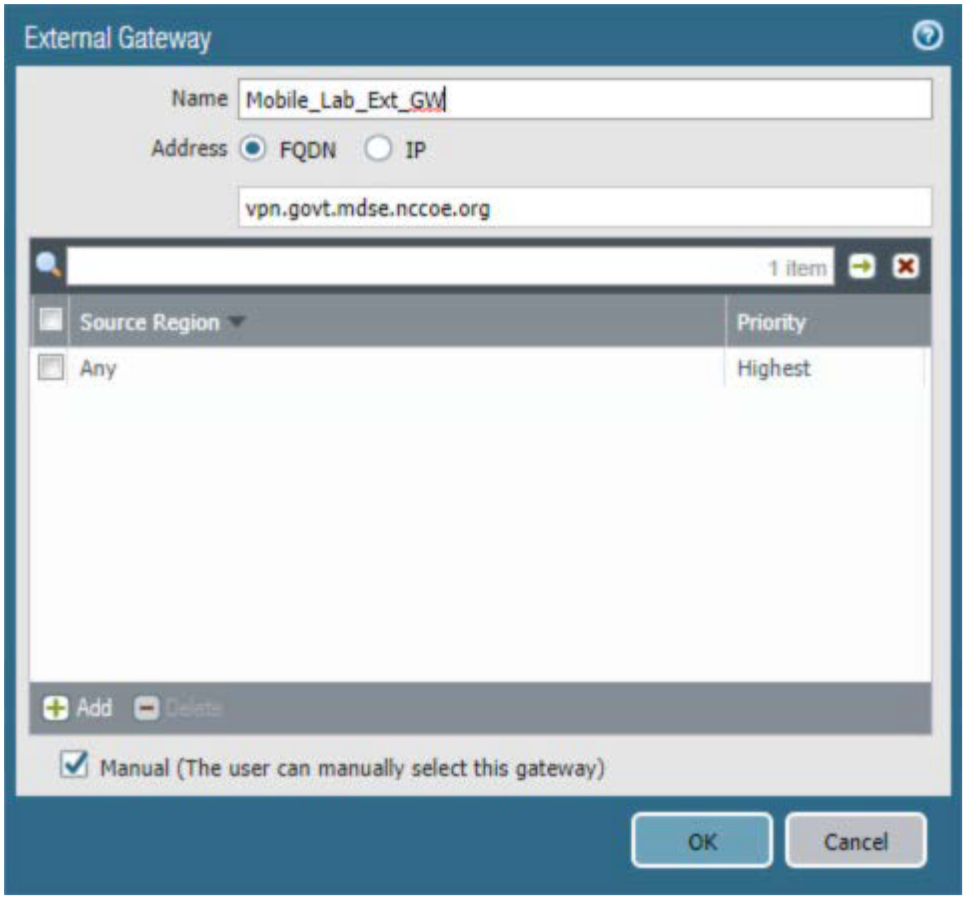
2) Dla opcji **Address** (Adres) wprowadź nazwę FQDN dla tego urządzenia. W tym przykładowym wdrożeniu nazwa FQDN to **vpn.govt.mdse.nccoe.org**.

3) Pod polem listy **Source Region** (Region źródłowy) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.

4) W nowej pozycji na liście **Source Region** (Region źródłowy) wybierz opcję **Any** (Dowolny).

5) Zaznacz pole wyboru **Manual** (Ręcznie).

6) Kliknij przycisk **OK**.



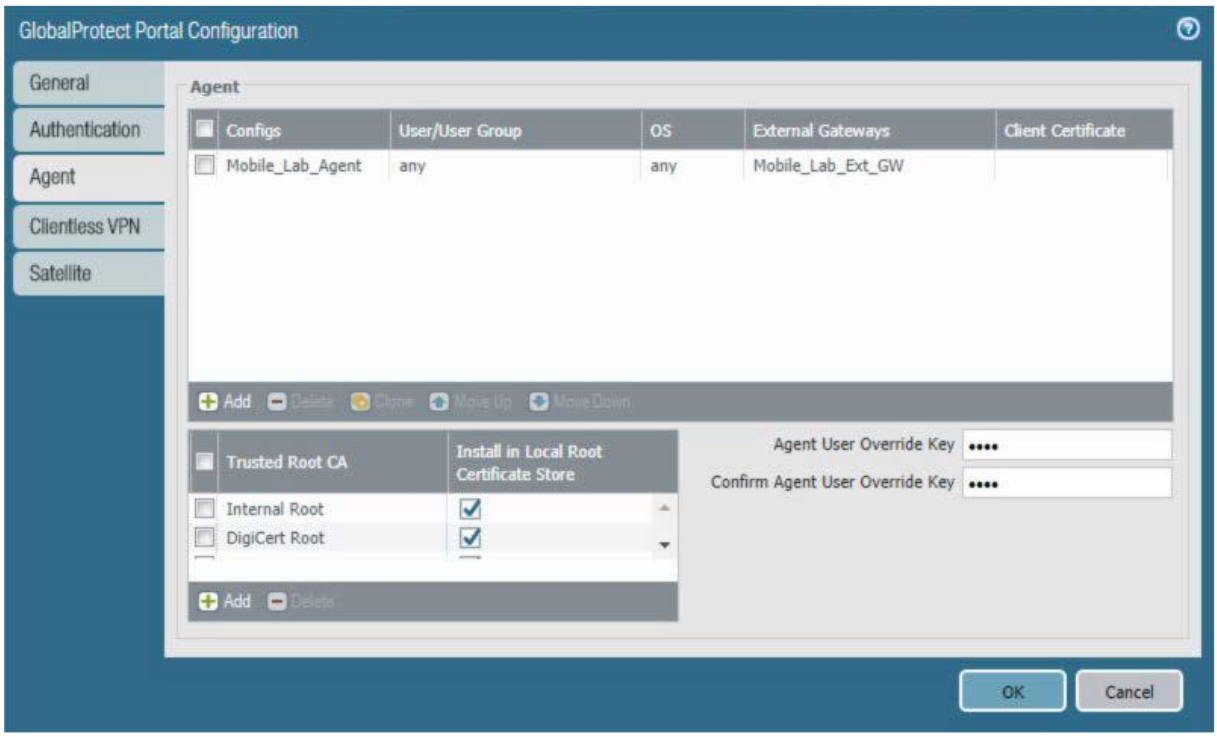
Rysunek 2-81 Konfiguracja bramy zewnętrznej GlobalProtect

iv. Pod polem listy **Trusted Root CA** (Zaufany główny CA) kliknij przycisk **Add** (Dodaj). Na liście pojawi się nowa pozycja.

v. W nowej pozycji na liście **Trusted Root CA** (Zaufany główny CA) wybierz swój wewnętrzny certyfikat od głównego CA.

vi. Powtórz kroki 7biii i 7biv, aby dodać wszystkie certyfikaty do wewnętrznych lub zewnętrznych łańcuchów zaufania wykorzystywanych, gdy urządzenia mobilne kontaktują się z portalem GlobalProtect.

c. Kliknij opcję **App** (Aplikacja). Upewnij się, że opcja **Connect Method** (Metoda połączenia) jest ustawiona na **User-logon (Always On)** [Logowanie użytkownika (zawsze włączone)].



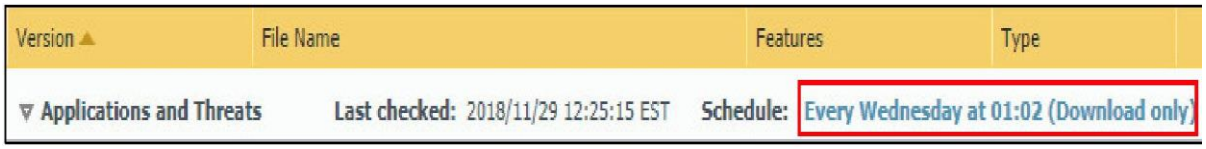
Rysunek 2-82 Konfiguracja agenta portalu GlobalProtect

d. Kliknij przycisk **OK**.

2.5.14. KONFIGUROWANIE AUTOMATYCZNYCH AKTUALIZACJI ZAGROŻEŃ I APLIKACJI

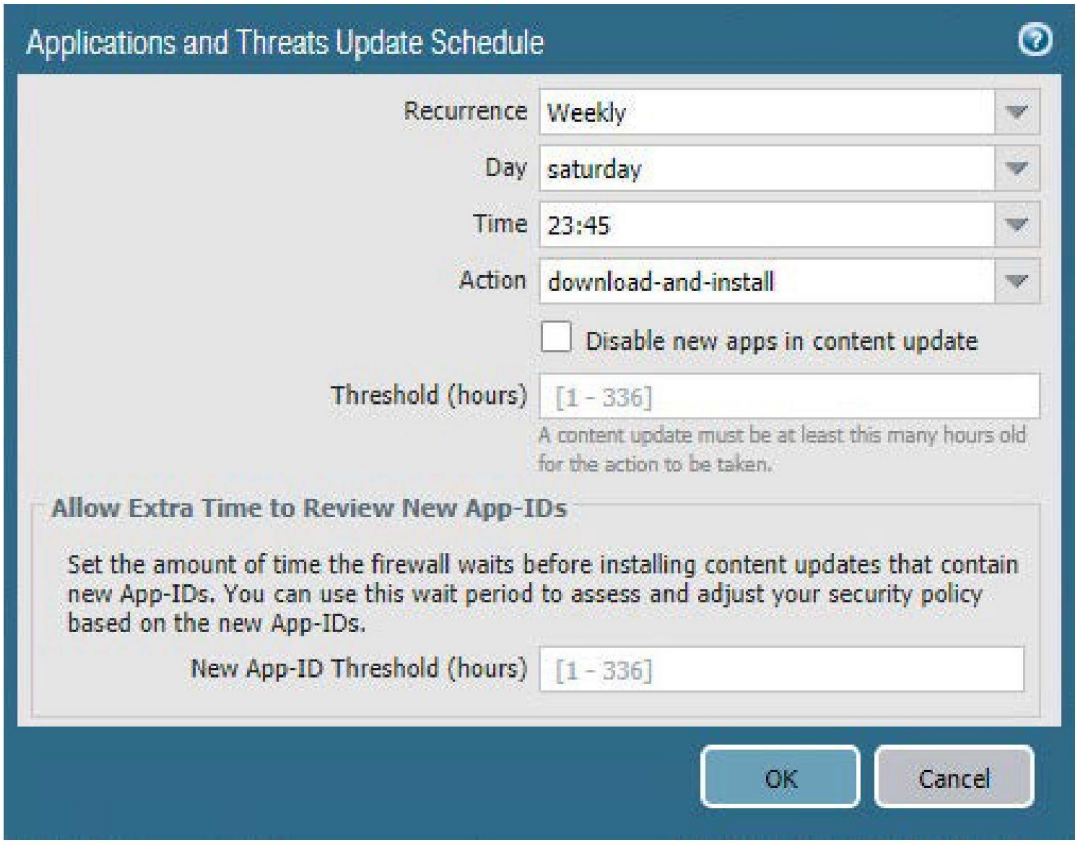
1. W portalu PAN-OS wybierz kolejno opcje **Device** (Urządzenie) > **Dynamic Updates** (Aktualizacje dynamiczne).

2. Kliknij przycisk **Check Now** (Sprawdź teraz) u dołu strony.
3. W części **Applications and Threats** (Aplikacje i zagrożenia) kliknij przycisk **Download** (Pobierz) obok ostatniej pozycji na liście z najpóźniejszą datą wydania. Pobranie aktualizacji może chwilę potrwać.
4. Po zakończeniu pobierania kliknij przycisk **Done** (Gotowe).
5. Kliknij przycisk **Install** (Zainstaluj) obok pobranej aktualizacji.
6. Kliknij przycisk **Continue Installation** (Kontynuuj instalację).
7. Po zakończeniu instalacji kliknij przycisk **Close** (Zamknij).
8. Następnie kliknij łącze z datą i godziną w opcji **Schedule** (Harmonogram).



Rysunek 2-83 Łącze do harmonogramu

9. Wybierz żądaną częstotliwość powtarzania. W tym wdrożeniu użyto opcji **Weekly** (Co tydzień).
10. Wybierz odpowiednią datę i godzinę. W przypadku tego wdrożenia zdecydowano się na aktualizacje w soboty o godzinie 23:45.
11. W polu **Action** (Akcja) wybierz opcję **download-and-install** (pobierz-i-zainstaluj).



Rysunek 2-84 Harmonogram aktualizacji zagrożeń

12. Kliknij przycisk **OK**.
13. W prawym górnym rogu kliknij przycisk **Commit** (Zatwierdź).
14. W oknie podręcznym kliknij przycisk **Commit** (Zatwierdź).

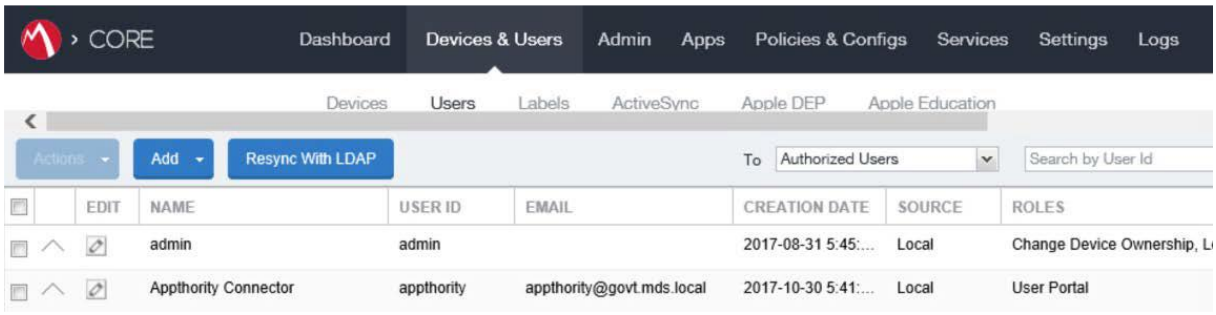
2.6. INTEGRACJA USŁUGI KRYPTOWIRE EMM+S Z SYSTEMEM MOBILEIRON

Usługa weryfikacji aplikacji Kryptowire wykorzystuje interfejs programistycznya aplikacji (API) systemu MobileIron do regularnego pobierania aktualnych informacji o spisie aplikacji na urządzeniach z systemu MobileIron Core. Zaktualizowane wyniki analizy są wyświetlane w portalu Kryptowire.

2.6.1. DODAWANIE KONTA W INTERFEJSIE API MOBILEIRON DLA USŁUGI KRYPTOWIRE

Poniższe kroki umożliwią utworzenie konta administracyjnego, które nada usłudze Kryptowire określone uprawnienia wymagane w systemie MobileIron.

1. Na stronie **MobileIron Admin Portal** przejdź do obszaru **Devices & Users** (Urządzenia i użytkownicy) > **Users** (Użytkownicy).
2. Na stronie **Users** (Użytkownicy):
    a. Wybierz opcje **Add** (Dodaj) > **Add Local User** (Dodaj użytkownika lokalnego). Zostanie otwarte okno dialogowe **Add New User** (Dodaj nowego użytkownika).



Rysunek 2-85 Użytkownicy systemu MobileIron

    b. W oknie dialogowym **Add New User** (Dodaj nowego użytkownika):
        i. W polu **User ID** (Identyfikator użytkownika) wprowadź tożsamość użytkownika, przy pomocy której będzie się uwierzytelniać usługa w chmurze Kryptowire. W naszym wdrożeniu użyto nazwy **kryptowire**.
        ii. W polu **First Name** (Imię) wprowadź ogólne imię dla usługi **Kryptowire**.
        iii. W polu **Last Name** (Nazwisko) wprowadź ogólne nazwisko dla usługi **Kryptowire**.

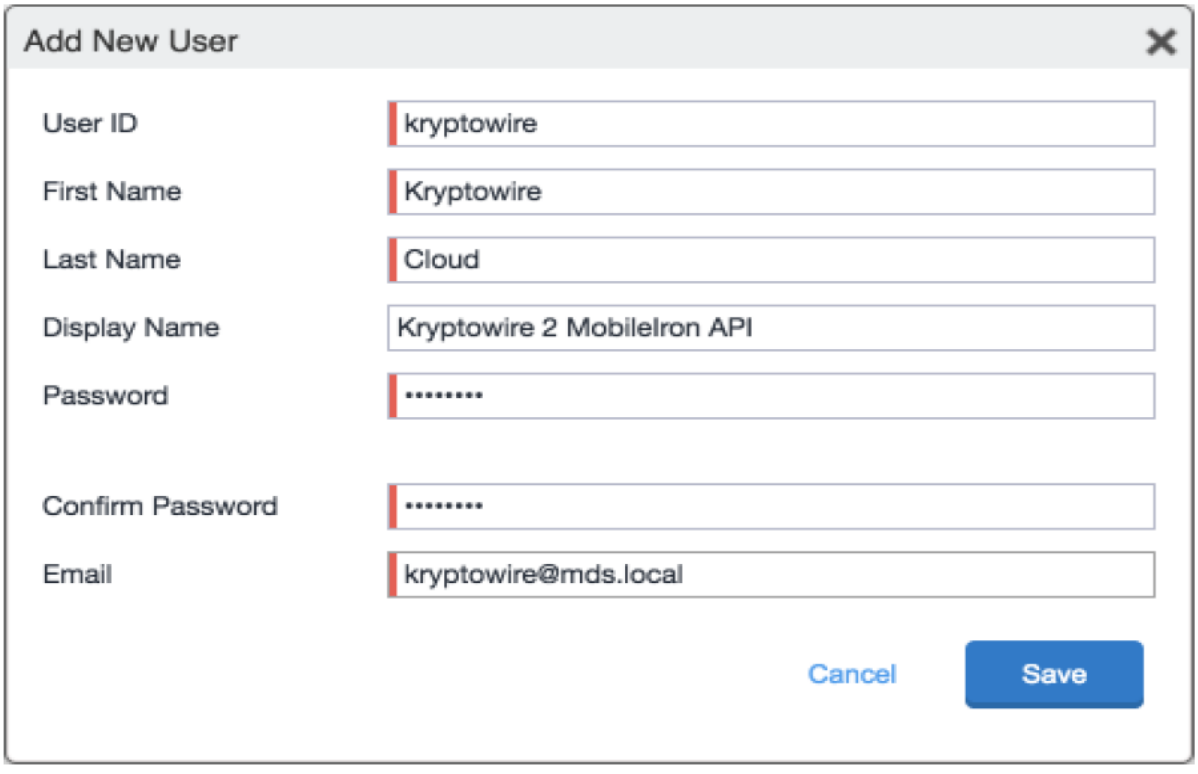
iv. W polu **Display Name** (Nazwa wyświetlana) można opcjonalnie wprowadzić nazwę wyświetlaną dla tego konta użytkownika.

v. W polu **Password** (Hasło) podaj hasło, którego tożsamość **Kryptowire** będzie używać do uwierzytelniania w systemie MobileIron.

vi. W polu **Confirm Password** (Potwierdź hasło) wprowadź to samo hasło, co w poprzednim kroku.

vii. W polu **Email** podaj konto e-mail dla tożsamości Kryptowire. Może ono być wykorzystane do konfigurowania automatycznych powiadomień i powinno być kontem kontrolowanym przez daną organizację.

viii. Kliknij przycisk **Save** (Zapisz).



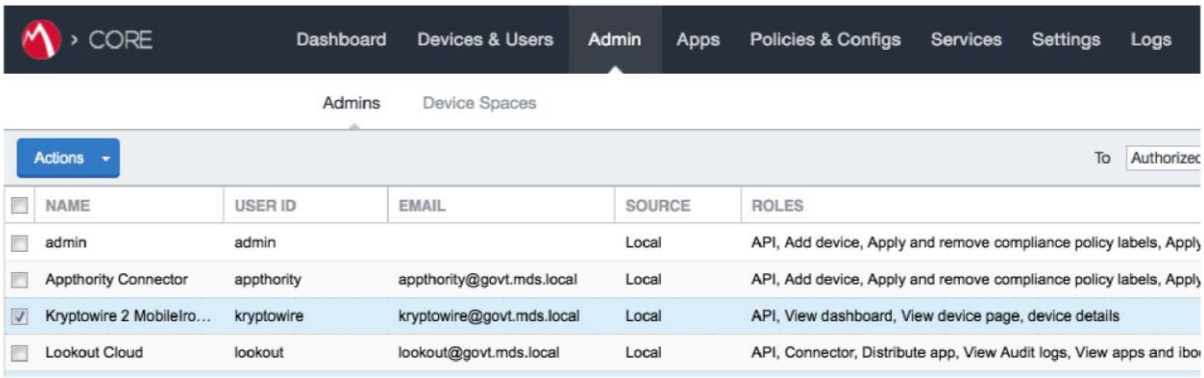
Rysunek 2-86 Konfiguracja użytkownika Kryptowire interfejsu API

3. Na stronie **MobileIron Admin Portal** przejdź do obszaru **Admin** (Administrator) > **Admins** (Administratorzy).

4. Na stronie **Admins** (Administratorzy):

    a. Zaznacz pole wyboru konta utworzonego dla usługi Kryptowire w kroku 2.

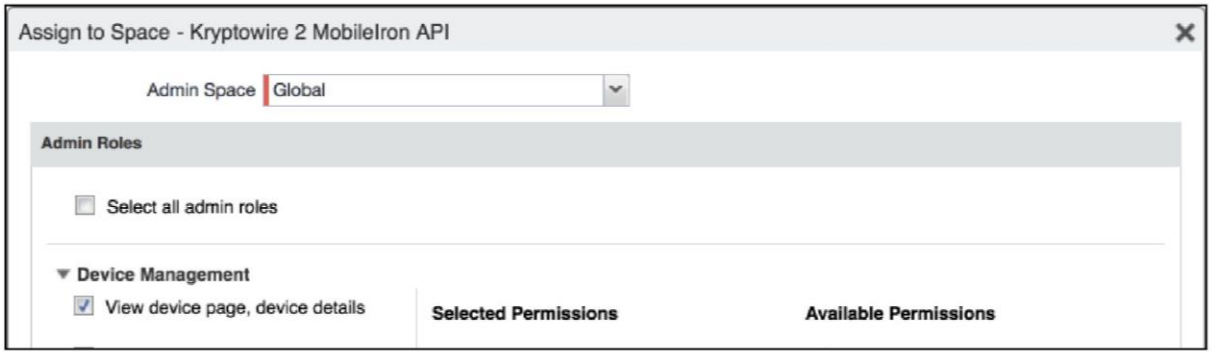
    b. Wybierz opcję **Actions** (Akcje) > **Assign to Space** (Przypisz do przestrzeni). Spowoduje to otwarcie okna dialogowego **Assign to Space** (Przypisz do przestrzeni) dla konta Kryptowire.



Rysunek 2-87 Lista użytkowników systemu MobileIron

    c. W oknie dialogowym **Assign to Space** (Przypisz do przestrzeni):

        i. Z menu rozwijanego **Select Space** (Wybierz przestrzeń) wybierz opcję **Global** (Globalna).



Rysunek 2-88 Przypisywanie przestrzeni do użytkownika Kryptowire interfejsu API

        ii. Włącz wszystkie poniższe ustawienia:

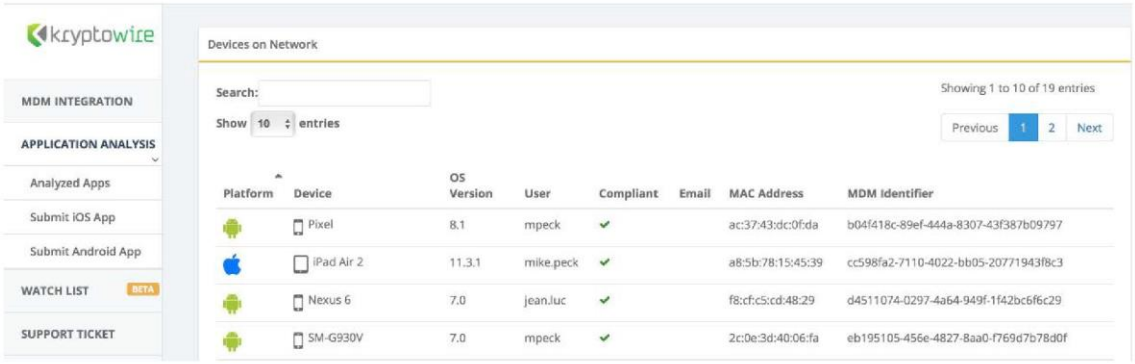
Admin Roles (Role administratora) > **Device Management** (Zarządzanie urządzeniami) > **View device page, device details** (Wyświetl stronę urządzenia, szczegóły urządzenia)

Admin Roles (Role administratora) > **Device Management** (Zarządzanie urządzeniami) > **View dashboard** (Wyświetl pulpit nawigacyjny)
Admin Roles (Role administratora) > **Privacy Control** (Kontrola prywatności) > **View apps and ibooks in device details** (Wyświetl aplikacje i pliki iBook w szczegółach urządzenia)
Admin Roles (Role administratora) > **Privacy Control** (Kontrola prywatności) > **View device IP and MAC address** (Wyświetl adres IP i MAC urządzenia)
Admin Roles (Role administratora) > **App Management** (Zarządzanie aplikacjami) > **View app** (Wyświetl aplikacje)
Admin Roles (Role administratora) > **App Management** (Zarządzanie aplikacjami) > **View app inventory** (Wyświetl spis aplikacji)
Other Roles (Inne role) > **Common Services Provider** (Dostawca usług wspólnych)
Other Roles (Inne role) > **API**

iii. Kliknij przycisk **Save** (Zapisz).

2.6.2. KONTAKT Z KRYPTOWIRE W CELU UTWORZENIA POŁĄCZENIA PRZYCHODZĄCEGO

Po utworzeniu konta API w systemie MobileIron skontaktuj się z obsługą klienta firmy Kryptowire, aby zintegrować swoją instancję systemu MobileIron Core. Należy pamiętać, że będzie to wymagało utworzenia reguł zapory, które zezwalają na połączenia przychodzące z adresów IP wskazanych przez usługę Kryptowire do systemu MobileIron Core przez port 443. Po nawiązaniu połączenia na stronie portalu Kryptowire pojawią się informacje o urządzeniach zarejestrowanych w systemie MobileIron. Identyfikator EMM prezentowany przez usługę Kryptowire będzie taki sam jak uniwersalny unikalny identyfikator przypisany do urządzenia przez system MobileIron Core.



Rysunek 2-89 Lista urządzeń w portalu Kryptowire

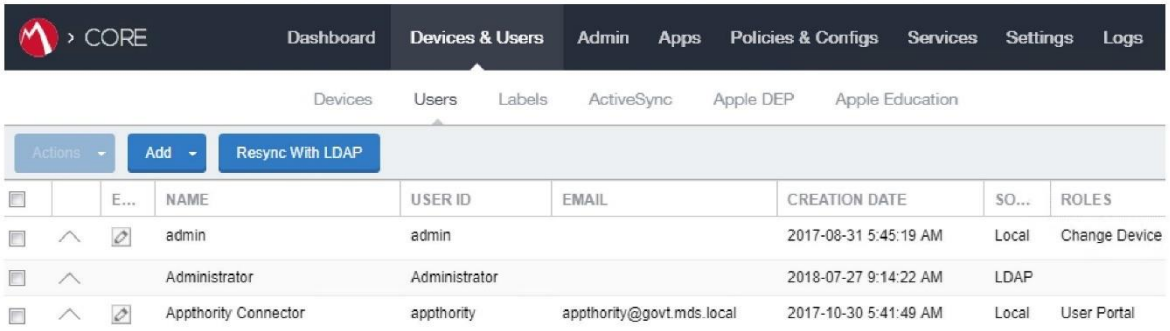
2.7. INTEGRACJA USŁUGI LOOKOUT MOBILE ENDPOINT SECURITY Z SYSTEMEM MOBILEIRON

Usługa w chmurze Mobile Endpoint Security firmy Lookout wykorzystuje interfejs API systemu MobileIron do pobierania szczegółowych informacji o urządzeniach mobilnych i spisu aplikacji z MobileIron Core. Po przeprowadzeniu analizy usługa Lookout wykorzystuje interfejs API, aby zastosować określone etykiety do urządzeń w celu ich skategoryzowania według ważności wykrytych problemów. System MobileIron można skonfigurować tak, aby automatycznie reagował na zastosowanie określonych etykiet w oparciu o wbudowane akcje zgodności.

2.7.1. DODAWANIE KONTA W INTERFEJSIE API MOBILEIRON DLA USŁUGI LOOKOUT

Poniższe kroki umożliwią utworzenie konta administracyjnego, które nada usłudze Lookout określone uprawnienia wymagane w systemie MobileIron.

1. Na stronie **MobileIron Admin Portal** przejdź do obszaru **Devices & Users** (Urządzenia i użytkownicy) > **Users** (Użytkownicy).
2. Na stronie **Users** (Użytkownicy):
   a. Wybierz opcje **Add** (Dodaj) > **Add Local User** (Dodaj użytkownika lokalnego). Zostanie otwarte okno dialogowe **Add New User** (Dodaj nowego użytkownika).



Rysunek 2-90 Lista użytkowników systemu MobileIron

b. W oknie dialogowym **Add New User** (Dodaj nowego użytkownika):

   i. W polu **User ID** (Identyfikator użytkownika) wprowadź tożsamość użytkownika, przy użyciu której będzie uwierzytelniana usługa w chmurze Lookout. W naszym wdrożeniu użyto nazwy **lookout**.

   ii. W polu **First Name** (Imię) wprowadź ogólne imię dla usługi **Lookout**.

   iii. W polu **Last Name** (Nazwisko) wprowadź ogólne nazwisko dla usługi **Lookout**.

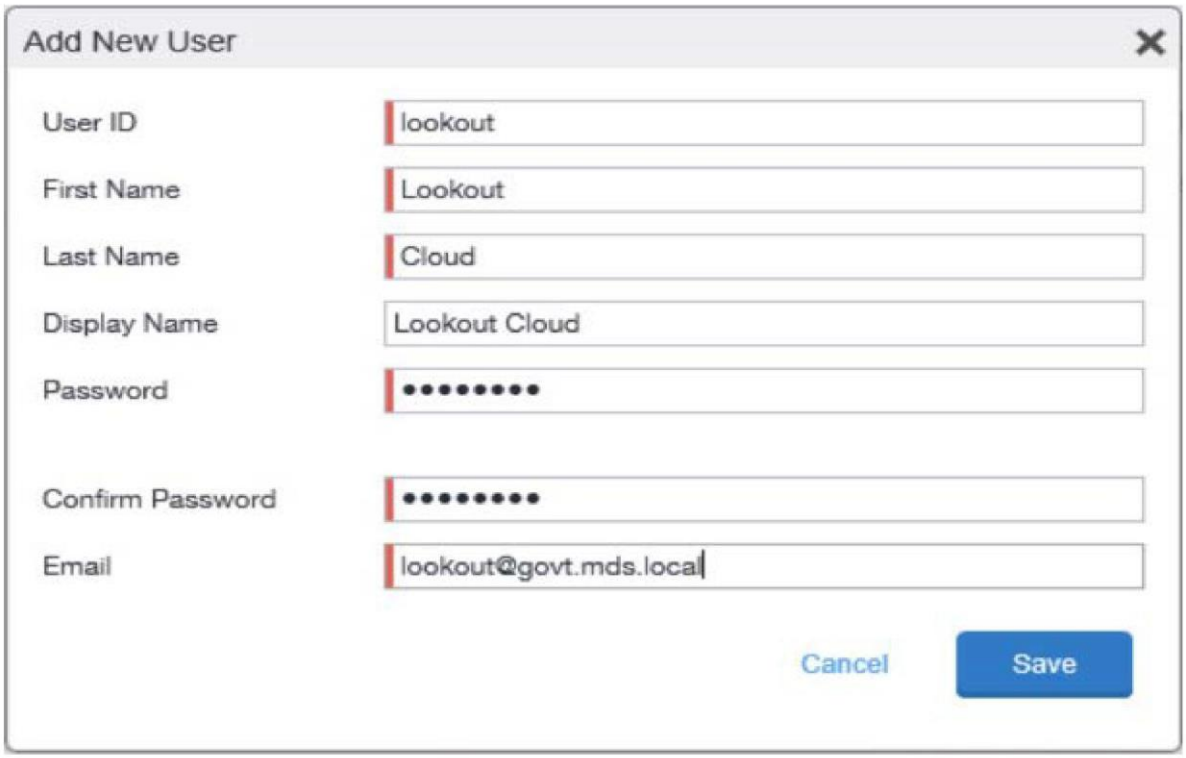
   iv. W polu **Display Name** (Nazwa wyświetlana) można opcjonalnie wprowadzić nazwę wyświetlaną dla tego konta użytkownika.

   v. W polu **Password** (Hasło) podaj hasło, którego tożsamość Lookout będzie używać do uwierzytelniania w systemie MobileIron.

   vi. W polu **Confirm Password** (Potwierdź hasło) wprowadź to samo hasło, co w poprzednim kroku.

   vii. W polu **Email** podaj konto e-mail dla tożsamości **Lookout**. Może ono być wykorzystywane do przesyłania alertów, dlatego powinno to być konto kontrolowane przez organizację.

   viii. Kliknij przycisk **Save** (Zapisz).



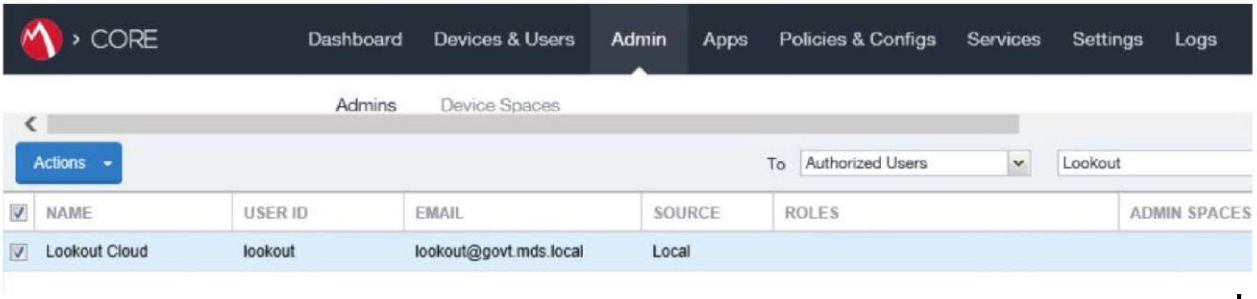
Rysunek 2-91 Konfiguracja użytkownika Lookout w systemie MobileIron

3. Na stronie **MobileIron Admin Portal** przejdź do części **Admin** (Administrator).

4. Na stronie **Admin** (Administrator):

   a. Zaznacz pole wyboru konta utworzonego dla usługi Lookout w kroku 2.

   b. Wybierz opcję **Actions** (Akcje) > **Assign to Space** (Przypisz do przestrzeni). Spowoduje to otwarcie okna dialogowego Assign to Space (Przypisz do przestrzeni) dla konta Lookout.

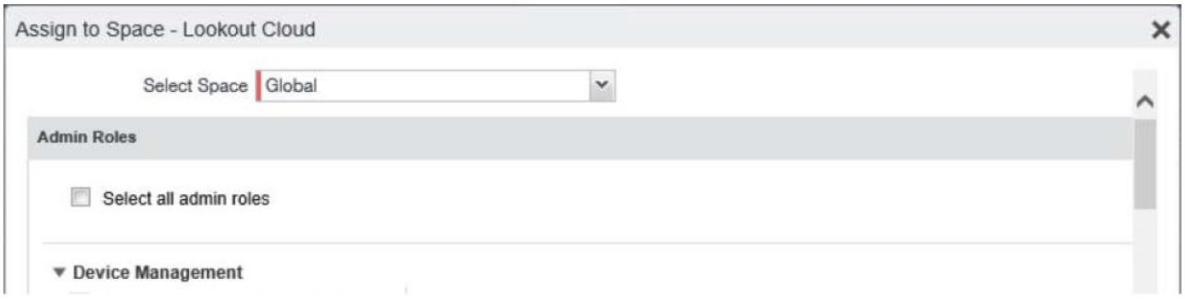


Rysunek 2-92 Konto administratora usługi Lookout w systemie MobileIron

Tłumaczenie

c. W oknie dialogowym **Assign to Space** (Przypisz do przestrzeni):

i. Z menu rozwijanego **Select Space** (Wybierz przestrzeń) wybierz opcję **Global** (Globalna).



Rysunek 2-93 Przypisywanie przestrzeni do konta usługi Lookout

ii. Włącz wszystkie poniższe ustawienia:

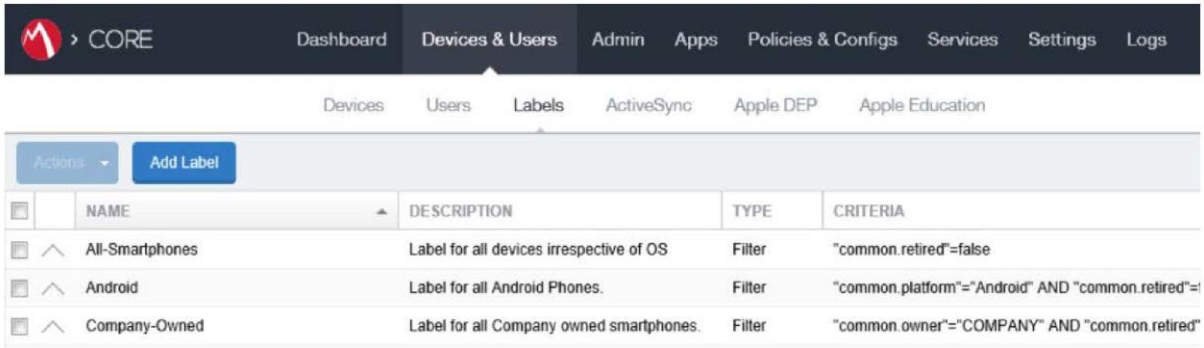
Admin Roles (Role administratora) > **Device Management** (Zarządzanie urządzeniami) > **View device page, device details** (Wyświetl stronę urządzenia, szczegóły urządzenia)
Admin Roles (Role administratora) > **Device Management** (Zarządzanie urządzeniami) > **View dashboard** (Wyświetl pulpit nawigacyjny)
Admin Roles (Role administratora) > **Label Management** (Zarządzanie etykietami) > **View label** (Wyświetl etykiety)
Admin Roles (Role administratora) > **Label Management** (Zarządzanie etykietami) > **Manage Label** (Zarządzaj etykietami)
Admin Roles (Role administratora) > **Privacy Control** (Kontrola prywatności) > **View apps and ibooks in device details** (Wyświetl aplikacje i pliki iBook w szczegółach urządzenia)
Admin Roles (Role administratora) > **Privacy Control** (Kontrola prywatności) > **View device IP and MAC address** (Wyświetl adres IP i MAC urządzenia)
Admin Roles (Role administratora) > **App Management** (Zarządzanie aplikacjami) > **Distribute app** (Udostępnij aplikacje)
Admin Roles (Role administratora) > **Logs and Event Management** (Zarządzanie dziennikami i zdarzeniami) > **View Audit logs** (Wyświetl dzienniki audytu)
Admin Roles (Role administratora) > **Logs and Event Management** (Zarządzanie dziennikami i zdarzeniami) > **View events** (Wyświetl zdarzenia)
Other Roles (Inne role) > **CSP**
Other Roles (Inne role) > **Connector** (Łącznik)
Other Roles (Inne role) > **API**

iii. Kliknij przycisk **Save** (Zapisz).

2.7.2. DODAWANIE ETYKIET W SYSTEMIE MOBILEIRON DLA USŁUGI LOOKOUT

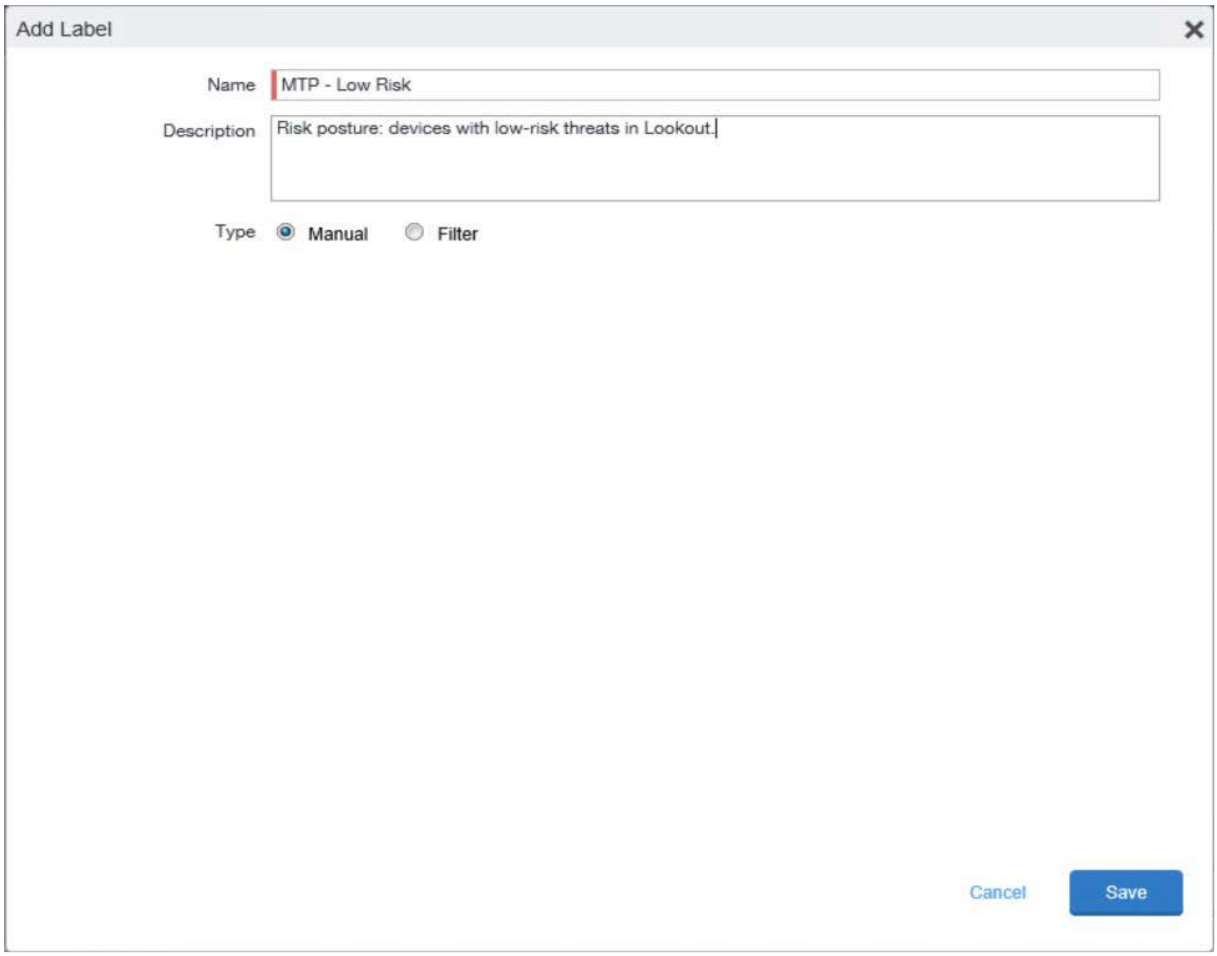
Usługa Lookout będzie dynamicznie przypisywać etykiety systemu MobileIron do chronionych urządzeń, aby informować o ich bieżącym stanie. Poniższe kroki umożliwią utworzenie grupy etykiet specyficznych dla usługi Lookout.

1. Na stronie **MobileIron Admin Portal** przejdź do obszaru **Devices & Users** (Urządzenia i użytkownicy) > **Labels** (Etykiety).
2. Na stronie **Labels** (Etykiety):
    a. Kliknij przycisk **Add Label** (Dodaj etykietę). Zostanie wyświetlone okno dialogowe **Add Label** (Dodaj etykietę).



Rysunek 2-94 Lista etykiet w systemie MobileIron

    b. W oknie dialogowym **Add Label** (Dodaj etykietę):
        i. W polu **Name** (Nazwa) wprowadź nazwę etykiety. Uwaga: w przyszłych krokach będą wykorzystywane przedstawione tutaj nazwy etykiet, ale ich stosowanie jest opcjonalne.
        ii. W polu **Description** (Opis) wprowadź krótki opis tej etykiety.
        iii. Dla ustawienia **Type** (Typ) wybierz opcję **Manual** (Ręczna). Spowoduje to ukrycie wszystkich pozostałych danych wejściowych formularza.
        iv. Kliknij przycisk **Save** (Zapisz).



Rysunek 2-95 Konfiguracja etykiety „MTP - Low Risk”

c. Wykonaj krok 2 dla każdej etykiety w poniższej tabeli:

Nazwa etykiety	Cel
Lookout for Work	Rejestracja urządzenia
MTP - Pending (MTP - oczekujące)	Zarządzanie cyklem życia: urządzenia, na których usługa Lookout nie została jeszcze aktywowana
MTP - Secured (MTP - zabezpieczone)	Zarządzanie cyklem życia: urządzenia, na których usługa Lookout została aktywowana
MTP - Threats Present (MTP - obecne zagrożenia)	Zarządzanie cyklem życia: urządzenia z zagrożeniami wykrytymi przez usługę Lookout
MTP Deactivated (MTP — dezaktywowano)	Zarządzanie cyklem życia: urządzenia, na których usługa Lookout została dezaktywowana

Nazwa etykiety	Cel
MTP Low Risk (MTP — niskie ryzyko)	Poziom ryzyka: urządzenia o niskiej ocenie ryzyka w usłudze Lookout
MTP Moderate Risk (MTP— umiarkowane ryzyko)	Poziom ryzyka: urządzenia o umiarkowanej ocenie ryzyka w usłudze Lookout
MTP High Risk (MTP — wysokie ryzyko)	Poziom ryzyka: urządzenia o wysokiej ocenie ryzyka w usłudze Lookout

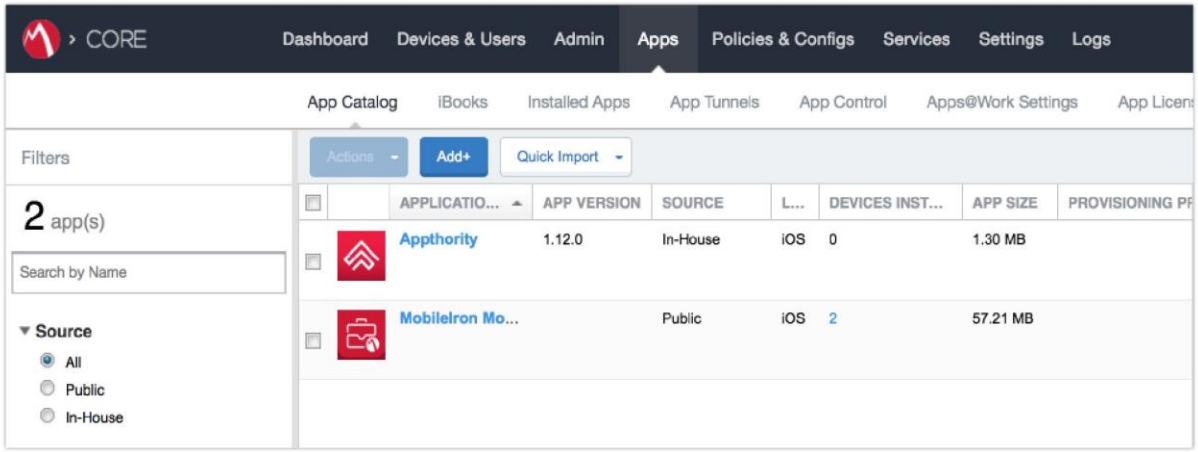
Uwaga: Administratorzy mogą zmieniać nazwy etykiet na bardziej odpowiednie dla ich środowiska.

2.7.3. DODAWANIE APLIKACJI LOOKOUT FOR WORK DLA SYSTEMU ANDROID DO KATALOGU APLIKACJI SYSTEMU MOBILEIRON

Poniższe kroki umożliwią dodanie aplikacji Lookout for Work dla systemu Android w systemie MobileIron.

1. Na stronie **MobileIron Admin Portal** przejdź do obszaru **Apps** (Aplikacje) > **App Catalog** (Katalog etykiet).

2. Na stronie **App Catalog** (Katalog aplikacji) kliknij przycisk **Add** (Dodaj). Spowoduje to rozpoczęcie procesu dodawania nowej aplikacji do katalogu.



Rysunek 2-96 Katalog aplikacji w systemie MobileIron

3. Na stronie **App Catalog** (Katalog aplikacji) > **Choose** (Wybierz):

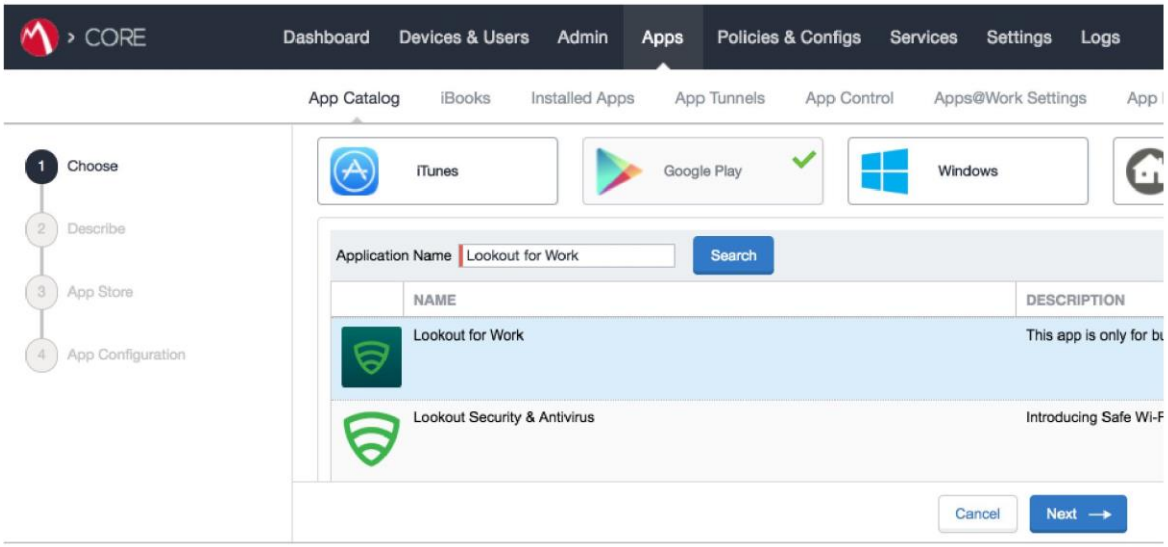
a. Zaznacz opcję **Google Play**. Zostaną wyświetlone dodatkowe elementy sterujące.

b. W polu **Application Name** (Nazwa aplikacji) wpisz **Lookout for Work**.

c. Kliknij przycisk **Search** (Szukaj). Wyniki wyszukiwania zostaną wyświetlone w dolnym obszarze.

d. Z listy wyników wyszukiwania wybierz aplikację **Lookout for Work**.

e. Kliknij przycisk **Next** (Dalej).

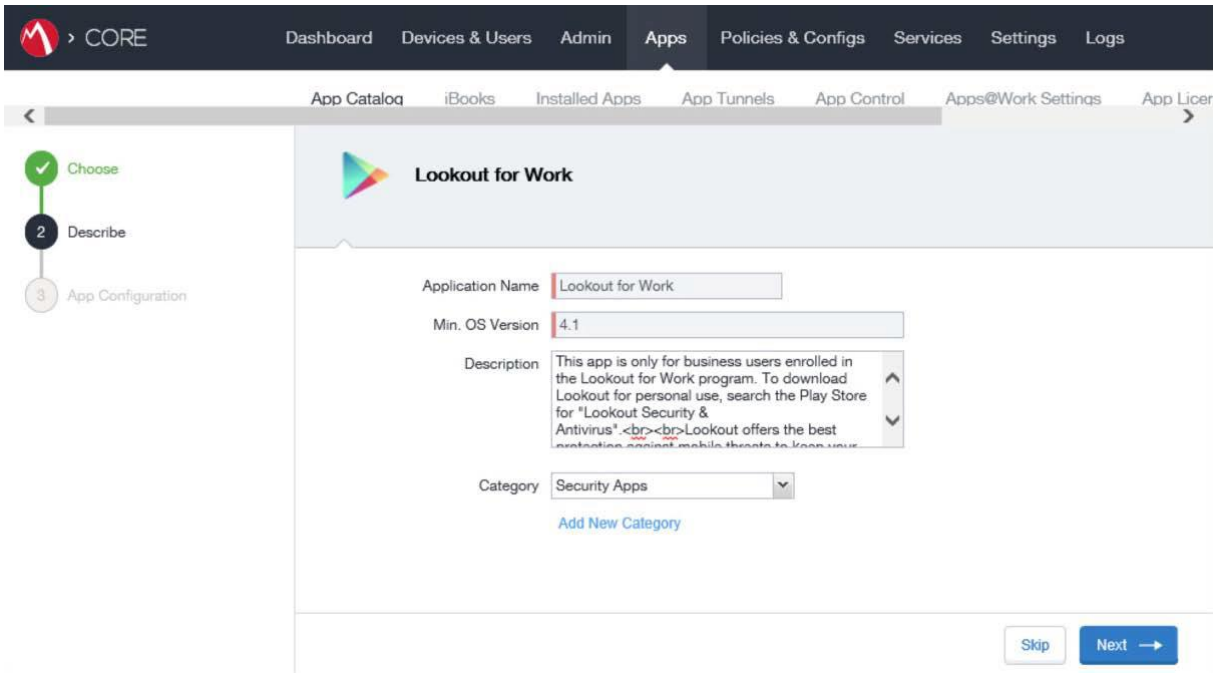


Rysunek 2-97 Dodawanie aplikacji Lookout for Work do katalogu aplikacji systemu MobileIron

4. Na stronie **App Catalog** (Katalog aplikacji) > **Describe** (Opisz):

a. W menu rozwijanym **Category** (Kategoria) opcjonalnie przypisz aplikację do kategorii odpowiedniej dla danej strategii wdrożenia systemu MobileIron.

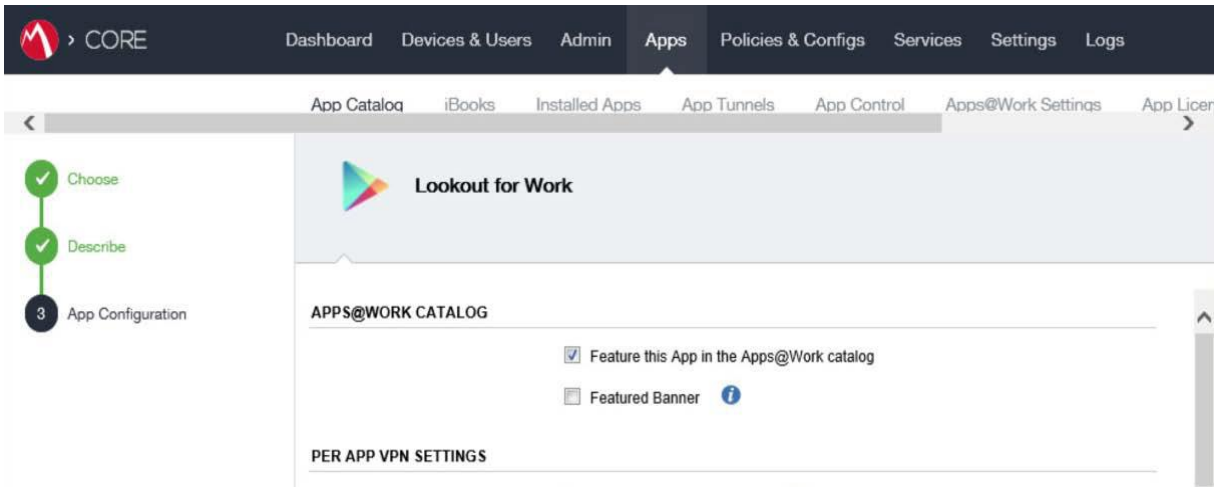
b. Kliknij przycisk **Next** (Dalej).



Rysunek 2-98 Konfiguracja aplikacji Lookout for Work

5. Na stronie **App Catalog** (Katalog aplikacji) > **App Configuration** (Konfiguracja aplikacji):

    a. W części **Apps@Work Catalog** (Katalog Apps@Work) włącz opcję **Feature this App in the Apps@Work catalog** (Włącz tę aplikację w katalogu Apps@Work).



Rysunek 2-99 Konfiguracja aplikacji Lookout for Work

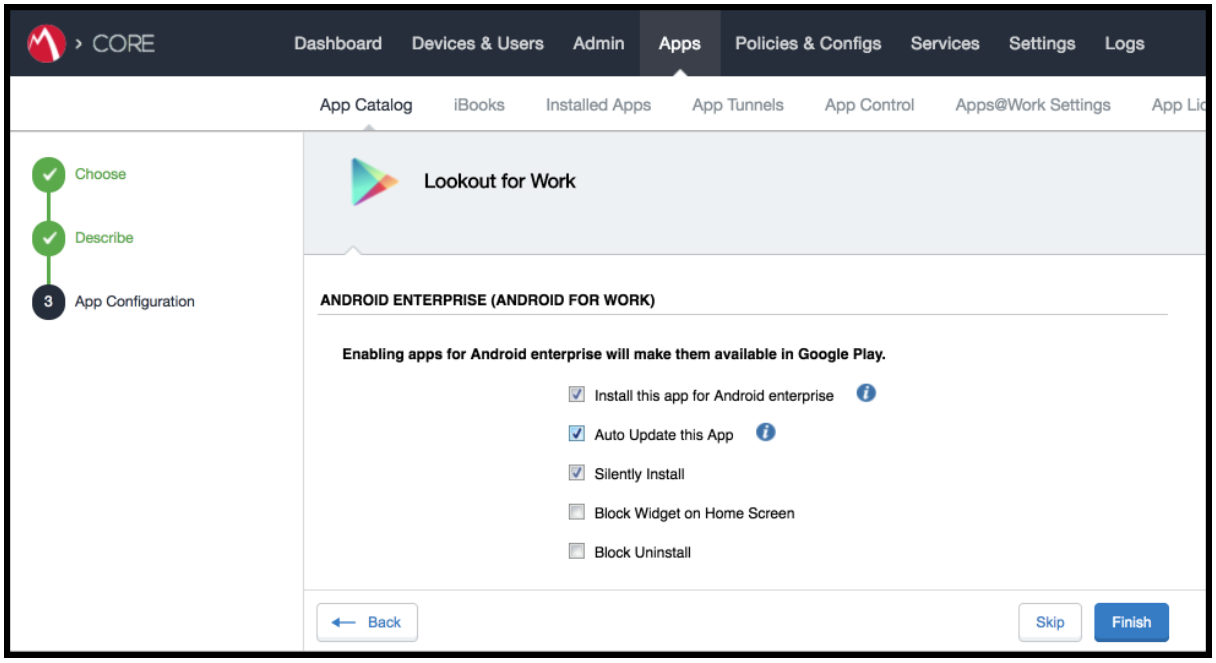
b. W obszarze **Android Enterprise** (Android for Work [AFW]):

i. Włącz opcję **Install this app for Android enterprise** (Zainstaluj tę aplikację dla systemu Android Enterprise). Zostaną wyświetlone dodatkowe element sterujące.

ii. Włącz opcję **Auto Update this App** (Automatycznie aktualizuj tę aplikację).

iii. Upewnij się, że opcja **Silently Install** (Cicha instalacja) jest włączona.

c. Kliknij przycisk **Finish** (Zakończ).



Rysunek 2-100 Konfiguracja aplikacji Lookout for Work dla systemu AWF

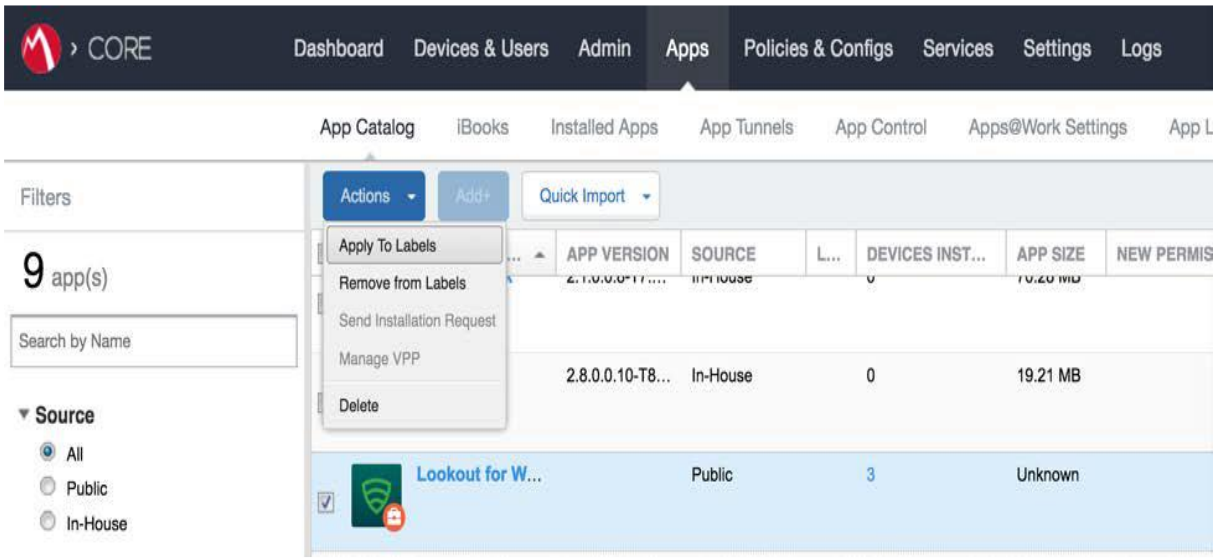
6. Aplikacja **Lookout for Work** powinna się teraz pojawić w katalogu aplikacji ze wskaźnikiem AFW.

2.7.4. STOSOWANIE ETYKIET DO APLIKACJI LOOKOUT FOR WORK DLA SYSTEMU ANDROID

1. Na stronie **App Catalog** (Katalog aplikacji):

a. Zaznacz aplikację Lookout for Work.

b. Wybierz opcje **Actions** (Akcje) > **Apply To Labels** (Zastosuj do etykiet). Zostanie wyświetlone okno dialogowe **Apply To Labels** (Zastosuj do etykiet).

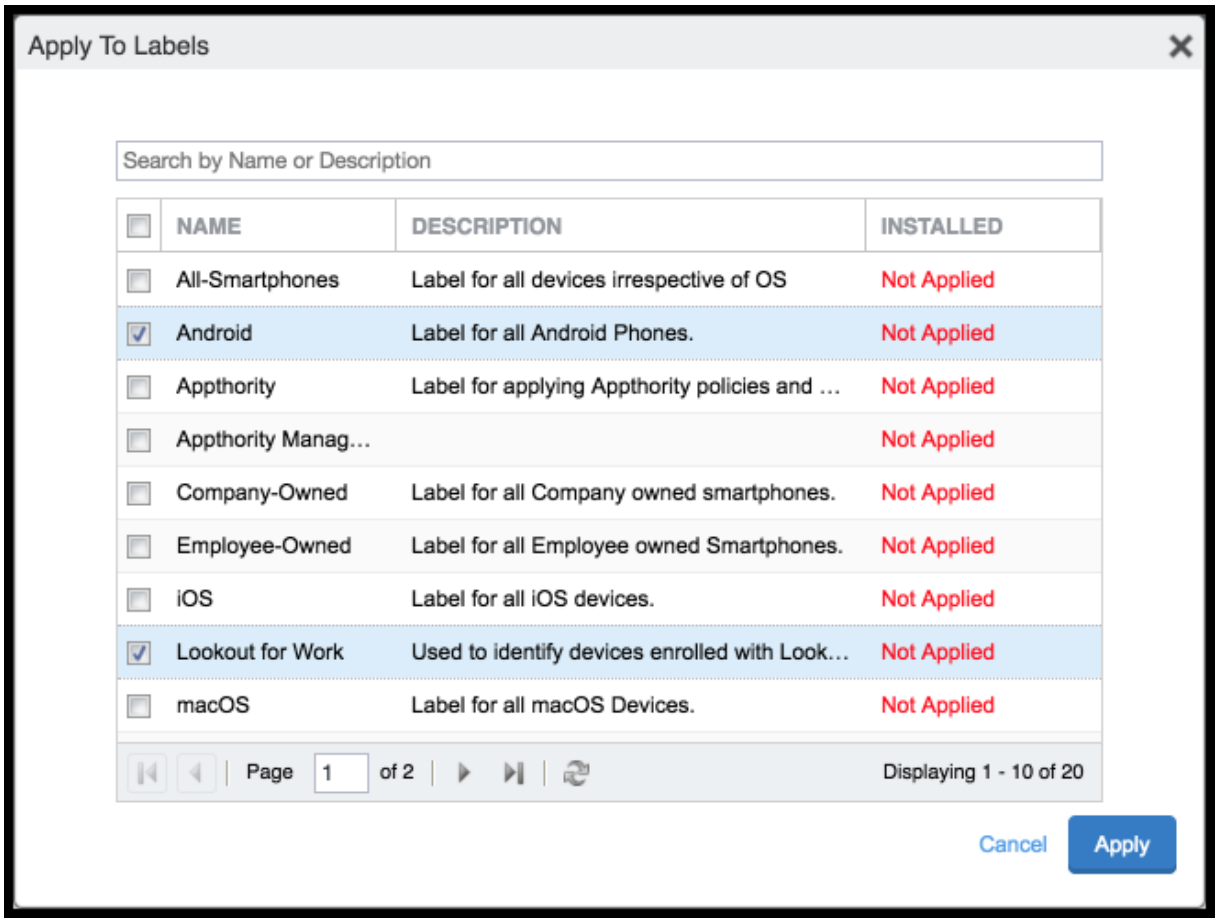


Rysunek 2-101 Zastosowanie aplikacji Lookout for Work do urządzeń z systemem Android

c. W oknie dialogowym **Apply To Labels** (Zastosuj do etykiet):

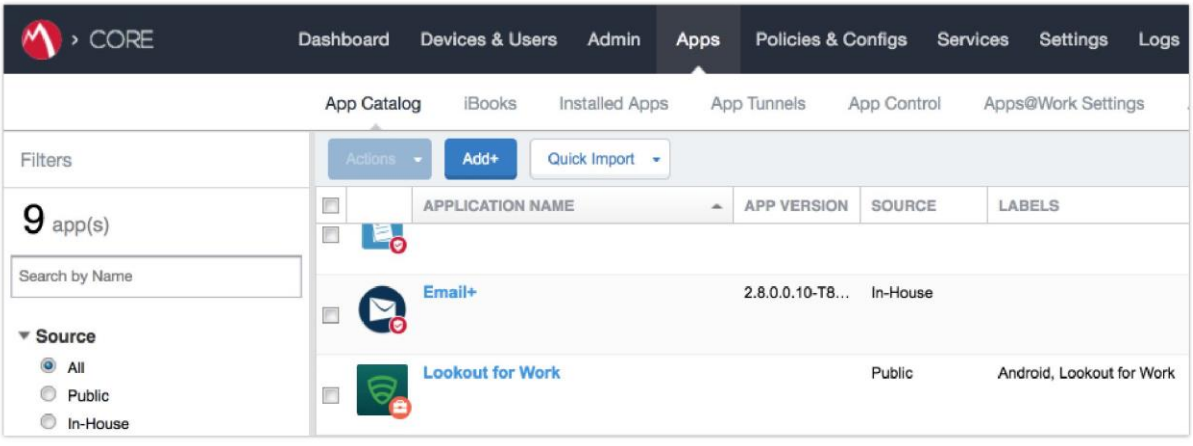
   i. Zaznacz etykiety aplikacji **Lookout for Work** i systemu **Android**, a także inne etykiety zgodne z zasadami bezpieczeństwa mobilnego w danej organizacji.

   ii. Kliknij przycisk **Apply** (Zastosuj).



Rysunek 2-102 Okno dialogowe Apply To Labels (Zastosuj do etykiet)

d. Aplikacja **Lookout for Work** zostanie wyświetlona z zastosowanymi etykietami **Lookout for Work** i **Android**.



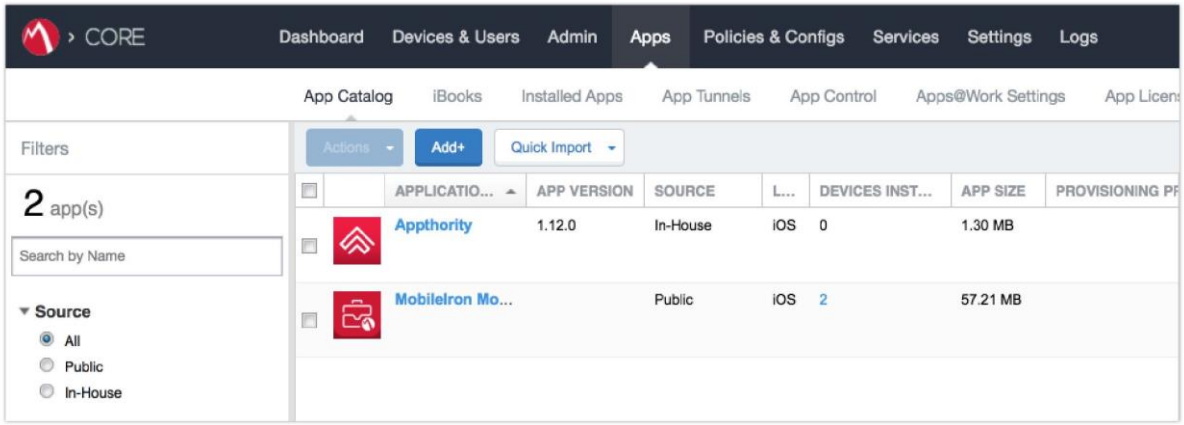
Rysunek 2-103 Aplikacja Lookout for Work z zastosowanymi etykietami

2.7.5. DODAWANIE APLIKACJI LOOKOUT FOR WORK DLA SYSTEMU IOS DO KATALOGU APLIKACJI SYSTEMU MOBILEIRON

Poniższe kroki umożliwiają dodanie aplikacji Lookout for Work dla systemu iOS do systemu MobileIron, zastosowanie odpowiednich etykiet MobileIron oraz utworzenie i przesłanie pliku konfiguracyjnego w celu aktywacji aplikacji jednym dotknięciem.

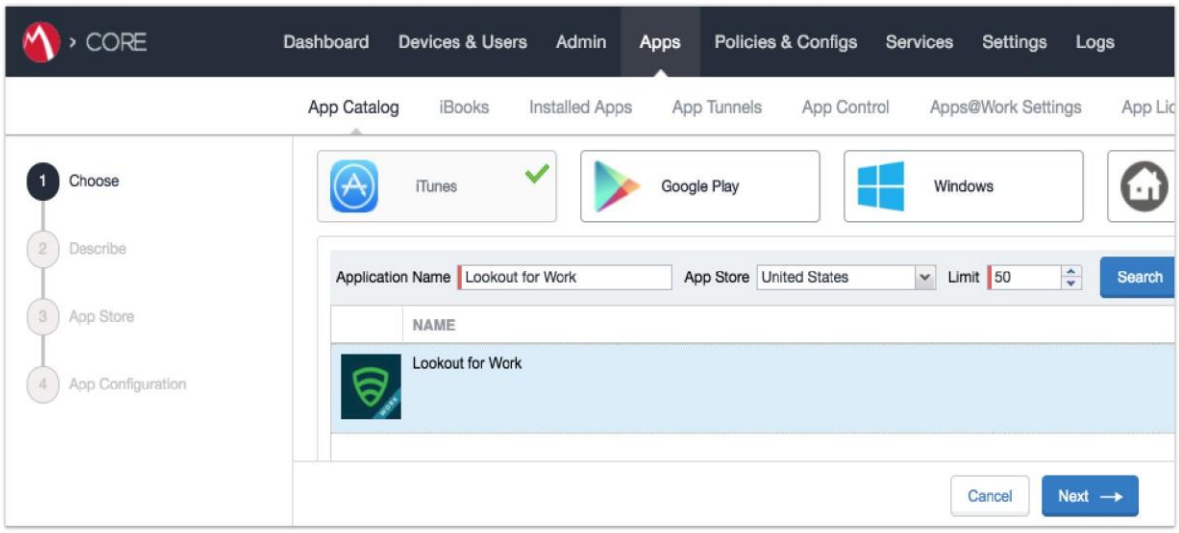
2.7.5.1. IMPORTOWANIE APLIKACJI LOOKOUT FOR WORK

1. Na stronie **MobileIron Admin Portal** przejdź do obszaru **Apps** (Aplikacje) > **App Catalog** (Katalog etykiet).
2. Na stronie **App Catalog** (Katalog aplikacji) kliknij przycisk **Add** (Dodaj). Spowoduje to rozpoczęcie procesu dodawania nowej aplikacji do katalogu.



Rysunek 2-104 Katalog aplikacji w systemie MobileIron

3. Na stronie **App Catalog** (Katalog aplikacji) > **Choose** (Wybierz):
   a. Zaznacz opcję **iTunes**. Zostaną wyświetlone dodatkowe elementy sterujące.
   b. W polu **Application Name** (Nazwa aplikacji) wpisz **Lookout for Work**.
   c. Kliknij przycisk **Search** (Szukaj). Wyniki wyszukiwania zostaną wyświetlone w dolnym obszarze.
   d. Z listy wyników wyszukiwania wybierz aplikację **Lookout for Work**.
   e. Kliknij przycisk **Next** (Dalej).

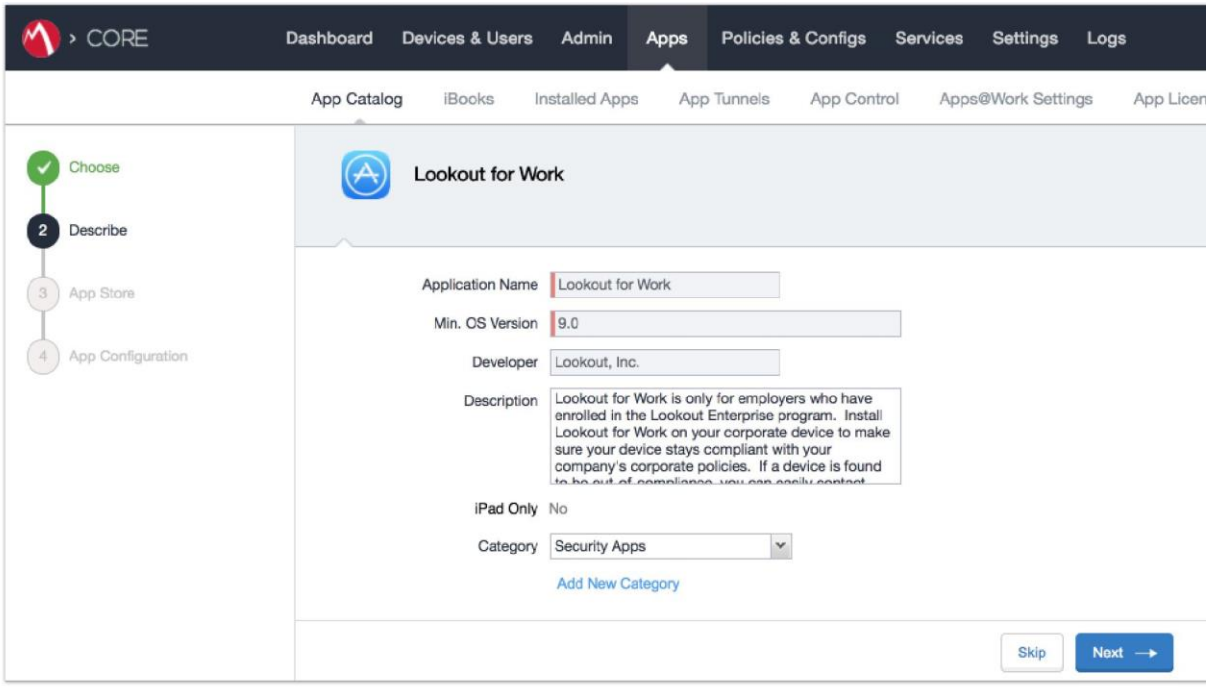


Rysunek 2-105 Aplikacja Lookout for Work wybrana ze sklepu iTunes

4. Na stronie **App Catalog** (Katalog aplikacji) > **Describe** (Opisz):

   a. W menu rozwijanym **Category** (Kategoria) opcjonalnie przypisz aplikację do kategorii odpowiedniej dla danej strategii wdrożenia systemu MobileIron.

   b. Kliknij przycisk **Next** (Dalej).



Rysunek 2-106 Konfiguracja aplikacji Lookout for Work

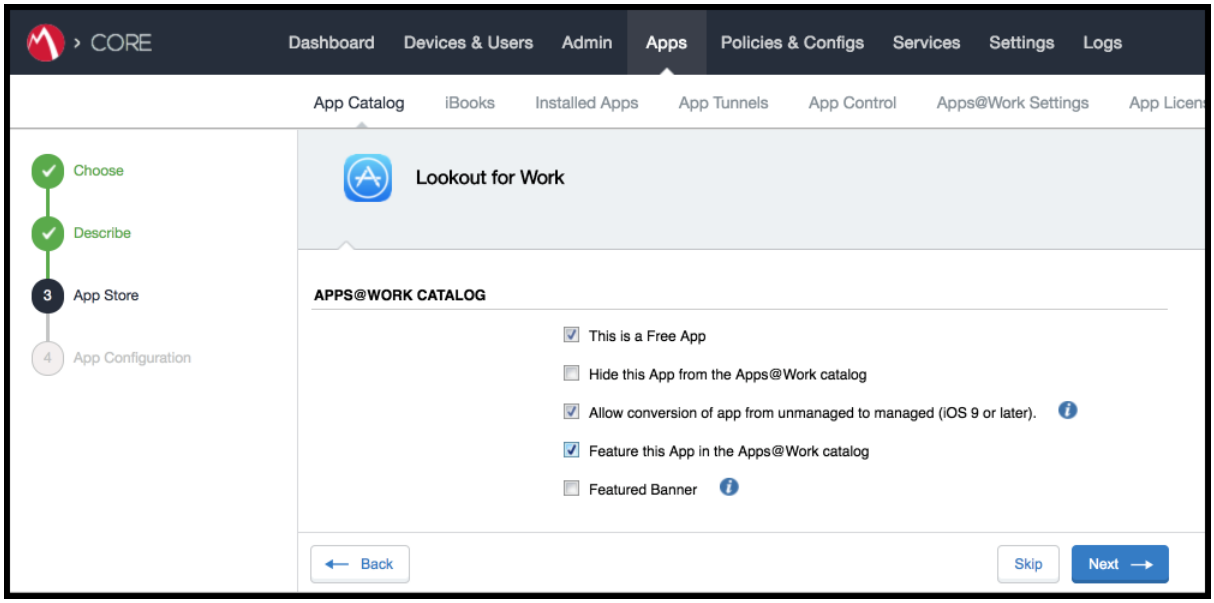
5. Na stronie **App Catalog** (Katalog aplikacji) > **App Store**:

    a. W obszarze **Apps@Work Catalog** (Katalog Apps@Work):

        i. Włącz opcję **Allow conversion of app from unmanaged to managed (iOS 9 or later)** [Włącz konwersję aplikacji z niezarządzanej na zarządzaną (iOS 9 lub nowszy)].

        ii. Włącz opcję **Feature this App in the Apps@Work catalog** (Włącz tę aplikację w katalogu Apps@Work).

        iii. Kliknij przycisk **Next** (Dalej).



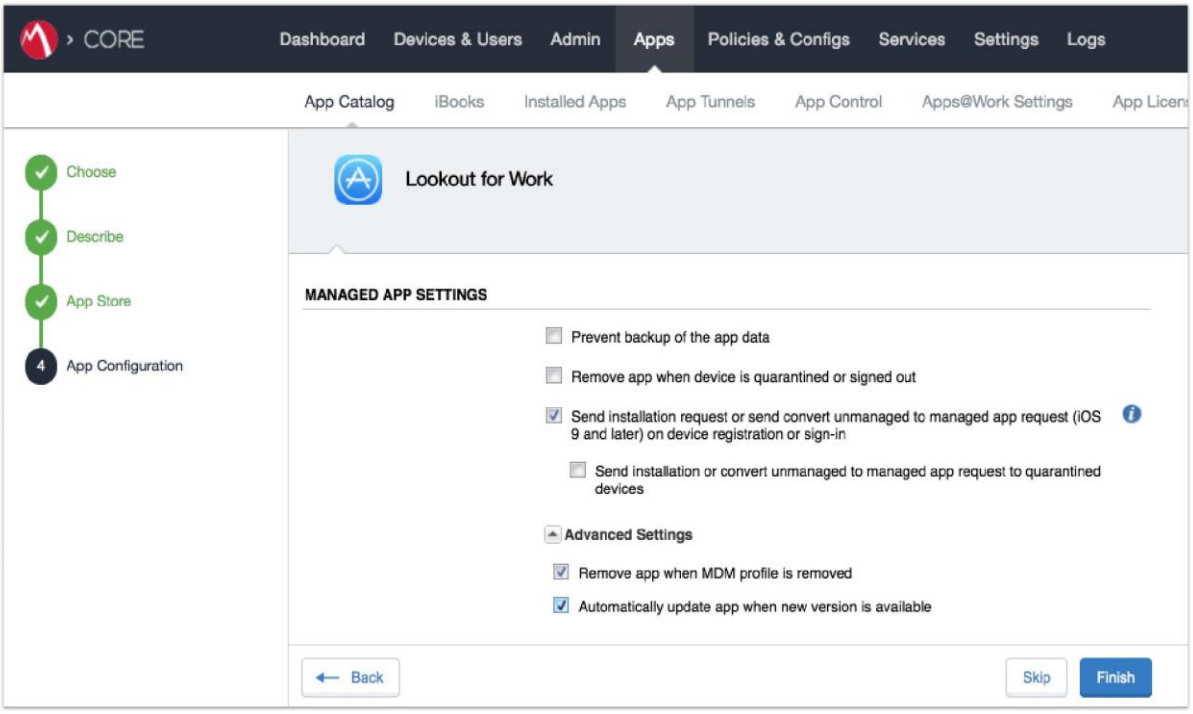
Rysunek 2-107 Konfiguracja aplikacji Lookout for Work

    b. W części **App Catalog** (Katalog aplikacji) > **App Configuration** (Konfiguracja aplikacji):

        i. Włącz opcję **Send installation request or send convert unmanaged to managed app request (iOS 9 and later) on device registration or sign-in.** [Wyślij żądanie instalacji lub żądanie konwersji aplikacji niezarządzanej na zarządzaną (iOS 9 lub nowszy) podczas rejestracji urządzenia lub logowania].

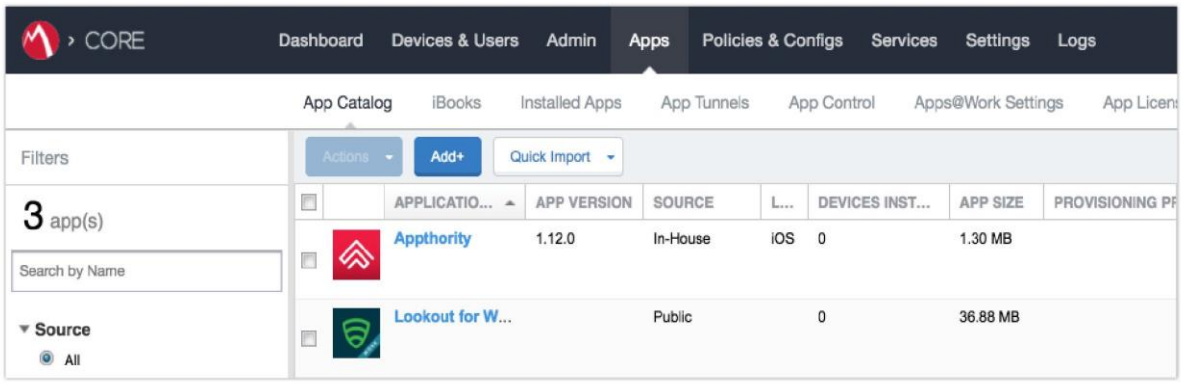
ii. Włącz opcję **Advanced Settings** (Ustawienia zaawansowane) > **Automatically update app when new version is available** (Automatycznie aktualizuj aplikację, gdy dostępna jest nowa wersja).

c. Kliknij przycisk **Finish** (Zakończ).



Rysunek 2-108 Ustawienia zarządzanej aplikacji Lookout for Work

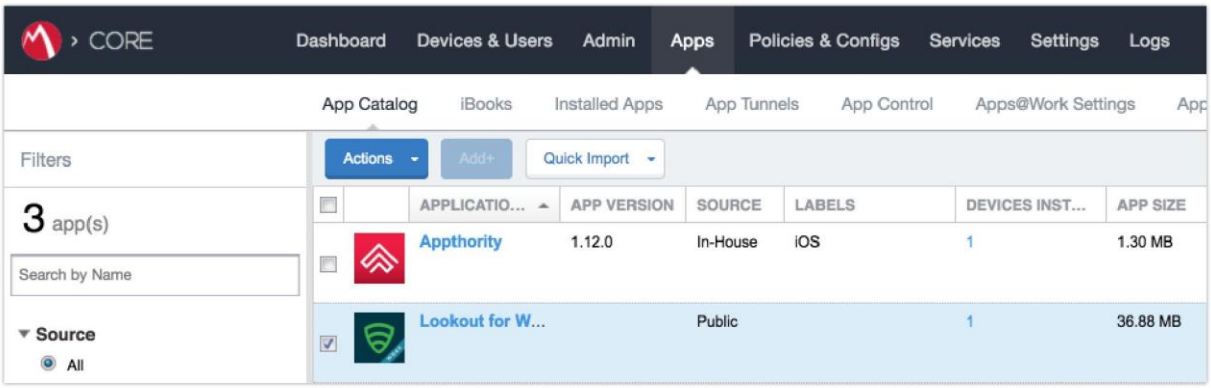
6. Aplikacja **Lookout for Work** powinna teraz pojawić się w katalogu aplikacji ze wskaźnikiem AFW.



Rysunek 2-109 Katalog aplikacji z aplikacją Lookout for Work

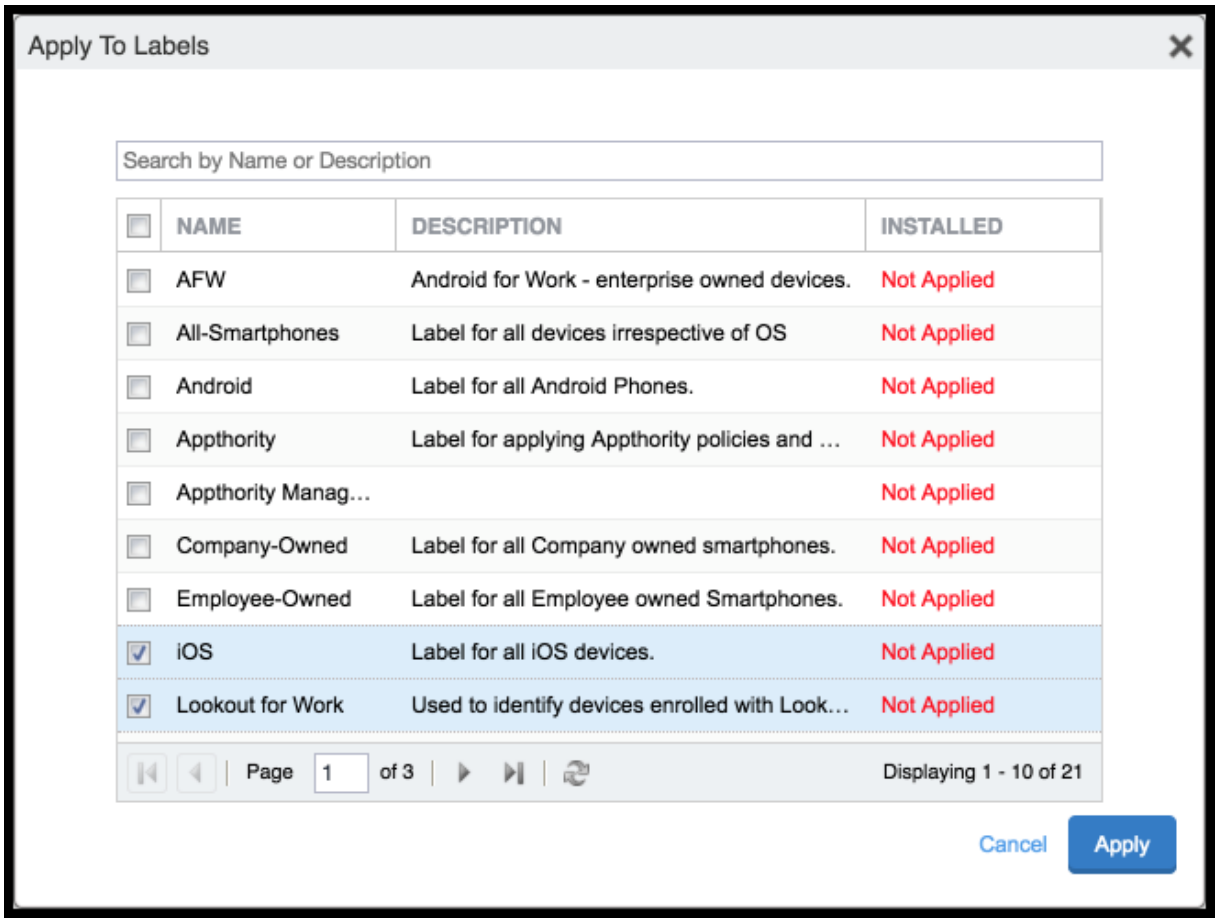
2.7.5.2. STOSOWANIE ETYKIET SYSTEMU MOBILEIRON DO APLIKACJI LOOKOUT FOR WORK

1. Na stronie **App Catalog** (Katalog aplikacji):
   a. Zaznacz aplikację **Lookout for Work**.
   b. Wybierz opcje **Actions** (Akcje) > **Apply To Labels** (Zastosuj do etykiet).
   Zostanie wyświetlone okno dialogowe **Apply To Labels** (Zastosuj do etykiet).



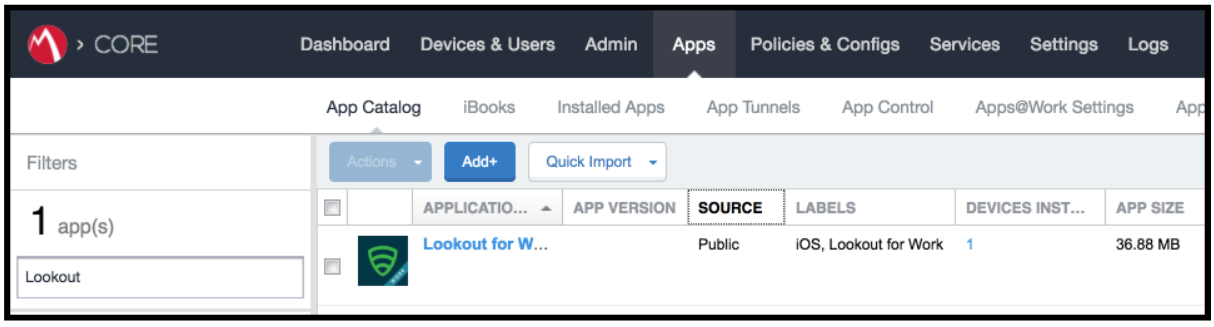
Rysunek 2-110 Wybrana aplikacja Lookout for Work

   c. W oknie dialogowym **Apply To Labels** (Zastosuj do etykiet):
      i. Zaznacz etykiety aplikacji **Lookout for Work** i systemu **iOS**, a także inne etykiety zgodne z zasadami bezpieczeństwa mobilnego w danej organizacji.
      ii. Kliknij przycisk **Apply** (Zastosuj).



Rysunek 2-111 Okno dialogowe Apply To Labels (Zastosuj do etykiet)

d. Aplikacja **Lookout for Work** zostanie wyświetlona z zastosowanymi etykietami Lookout for iOS.



Rysunek 2-112 Katalog aplikacji z aplikacją Lookout for Work

Tłumaczenie

2.7.5.3. TWORZENIE PLIKU KONFIGURACJI ZARZĄDZANEJ APLIKACJI DLA LOOKOUT FOR WORK

MobileIron może przesłać plik konfiguracyjny do zarządzanych urządzeń iOS, aby umożliwić użytkownikom aktywowanie aplikacji Lookout for Work. Poniższe kroki umożliwiają utworzenie i przesłanie niezbędnego pliku.

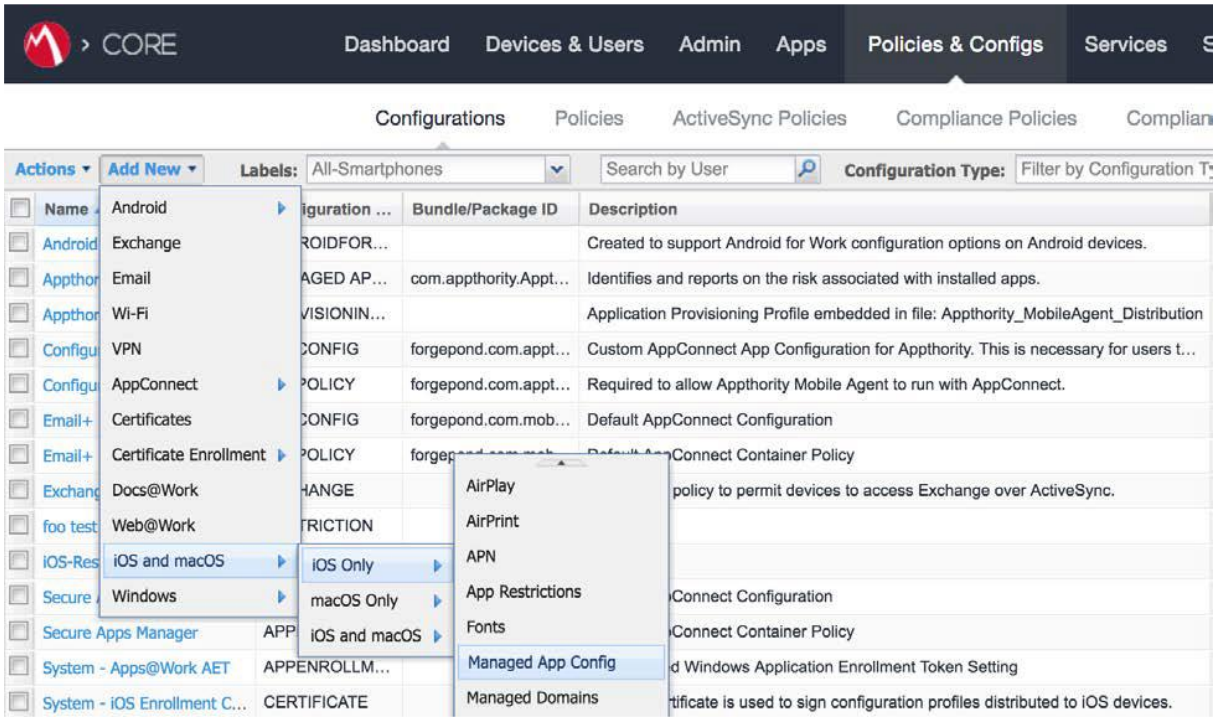
1. Korzystając ze **zwykłego edytora tekstowego**, utwórz następujący plik tekstowy, **zastępując gwiazdki w wierszu 13** globalnym kodem rejestracyjnym organizacji.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"https://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>MDM</key>
<string>MOBILEIRON</string>
<key>DEVICE_UDID</key>
<string>$DEVICE_UDID$</string>
<key>EMAIL</key>
<string>$EMAIL$</string>
<key>GLOBAL_ENROLLMENT_CODE</key>
<string>*******</string>
<dict>
</plist>
```

2. Na stronie **MobileIron Core Admin Portal** przejdź do obszaru **Policies & Configs** (Zasady i konfiguracja) > **Configurations** (Konfiguracje).

3. Na stronie **Configurations** (Konfiguracje):

    a. Wybierz kolejno opcje **Add New** (Dodaj nowy) > **iOS and OS** X (iOS i OS X) > **iOS Only** (Tylko iOS) > **Managed App Config** (Konfiguracja aplikacji zarządzanej). Zostanie otwarte okno dialogowe **New Managed App Config Setting** (Ustawienia konfiguracji nowej aplikacji zarządzanej).



Rysunek 2-113 Importowanie konfiguracji aplikacji zarządzanej

    b. W oknie dialogowym **Managed App Config Setting** (Ustawienia konfiguracji aplikacji zarządzanej):

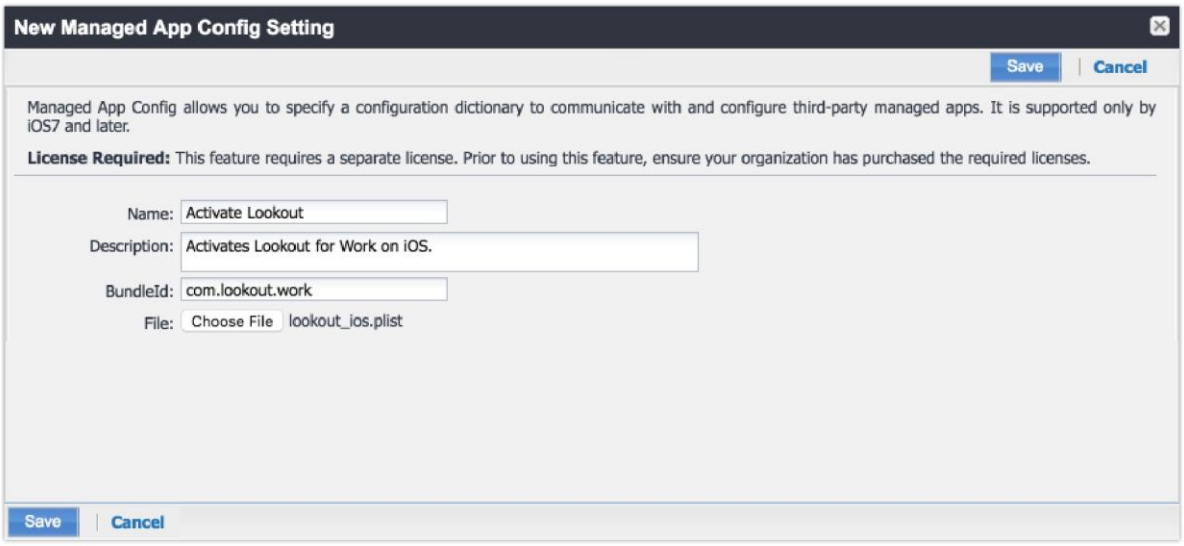
        i. W polu **Name** (Nazwa) wprowadź nazwę tej konfiguracji. W naszym wdrożeniu użyto nazwy **Activate Lookout** (Aktywuj Lookout).

        ii. W polu **Description** (Opis) podaj cel utworzenia tej konfiguracji.

        iii. W polu **BundleId** (Powiązane) wprowadź identyfikator pakietu aplikacji Lookout at Work — w przypadku naszej wersji to **com.lookout.work**.

iv. Wybierz opcję **Choose File...** (Wybierz plik...), aby przesłać plik plist[10] utworzony w kroku 1.

v. Kliknij przycisk **Save** (Zapisz).



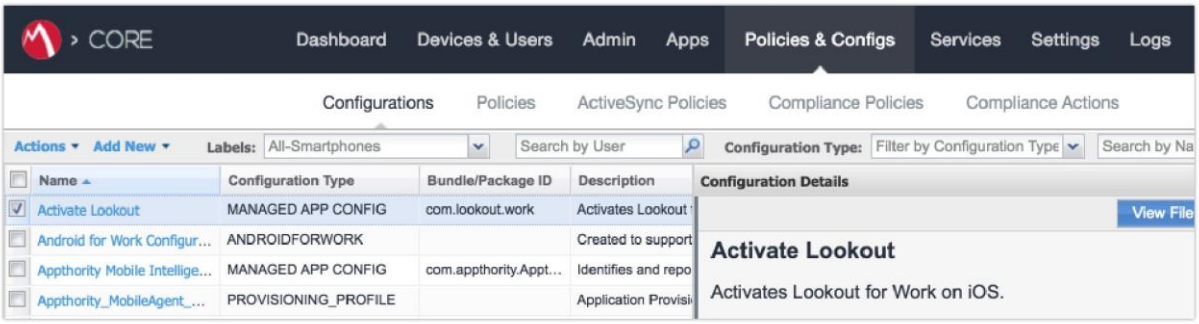
Rysunek 2-114 Konfiguracja pliku plist

2.7.5.4. STOSOWANIE ETYKIET DO KONFIGUROWANIA APLIKACJI ZARZĄDZANEJ DLA LOOKOUT FOR WORK

Poniższe kroki umożliwiają zastosowanie konfiguracji aplikacji zarządzanej utworzonej w poprzednim punkcie do etykiet.

1. Na stronie **MobileIron Core Admin Portal** przejdź do obszaru **Policies & Configs** (Zasady i konfiguracja) > **Configurations** (Konfiguracje).
2. Na stronie **Configurations** (Konfiguracje):
   a. Zaznacz konfigurację aplikacji zarządzanej **Lookout Activation** utworzoną w poprzednim punkcie.
   b. Wybierz opcje **Actions** (Akcje) > **Apply To Label** (Zastosuj do etykiety). Zostanie wyświetlone okno dialogowe **Apply To Label** (Zastosuj do etykiety).

[10] Property list - Lista właściwości

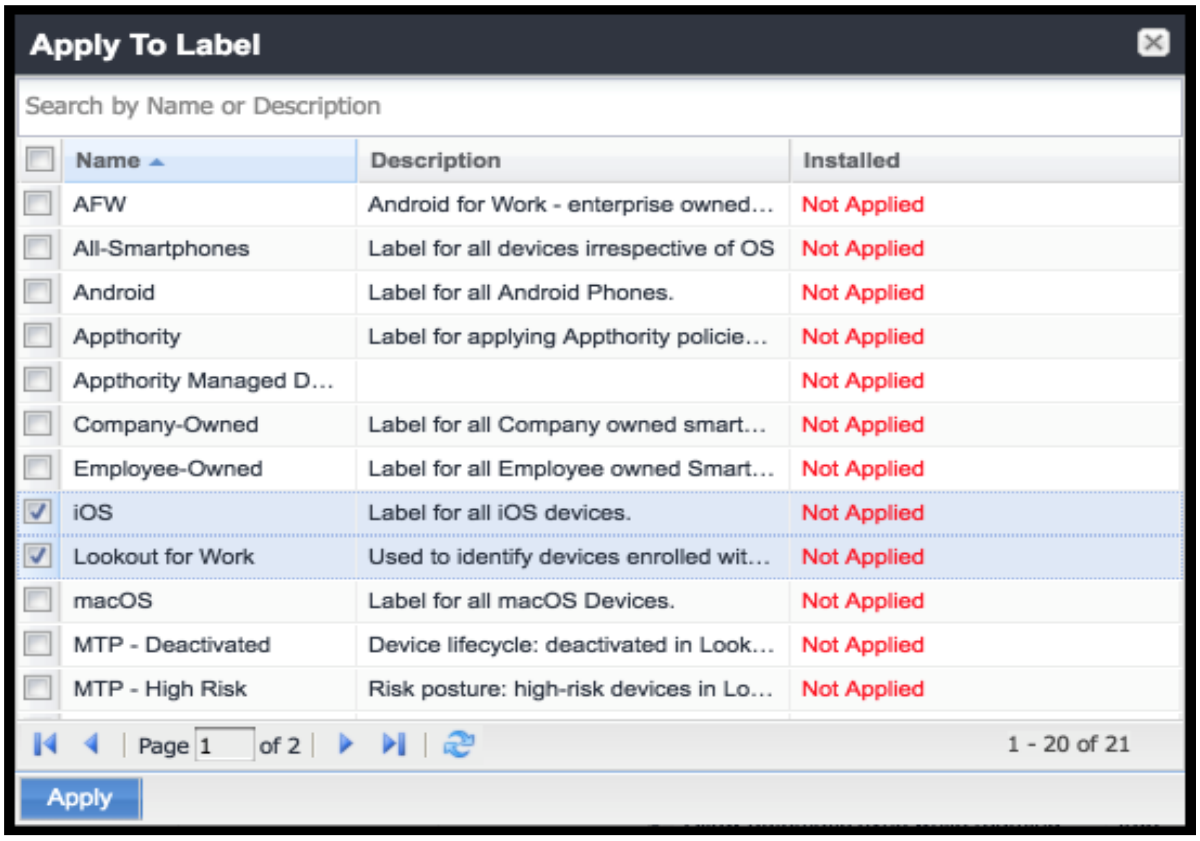


Rysunek 2-115 Wybrana konfiguracja aplikacji Lookout

c. W oknie dialogowym **Apply To Label** (Zastosuj do etykiety):

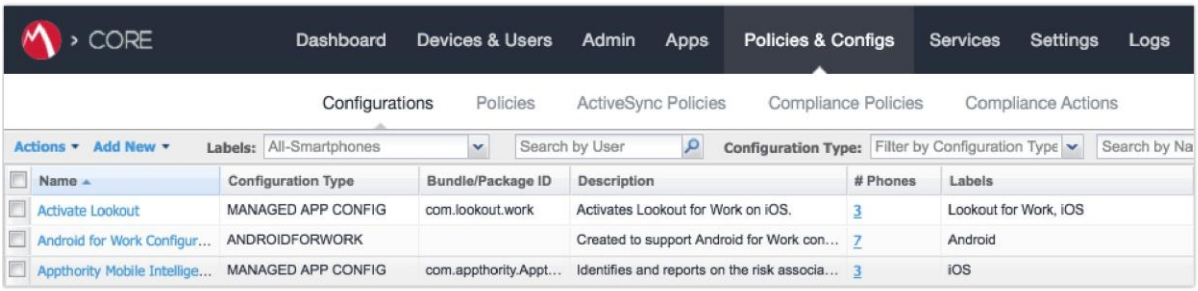
   i. Zaznacz etykiety **iOS** i **Lookout for Work**.

   ii. Kliknij przycisk **Apply** (Zastosuj).



Rysunek 2-116 Okno dialogowe Apply To Label (Zastosuj do etykiety)

d. W systemie powinno być teraz widoczne, że etykiety **Lookout for Work** i **iOS** zostały zastosowane do konfiguracji **Activate Lookout**.

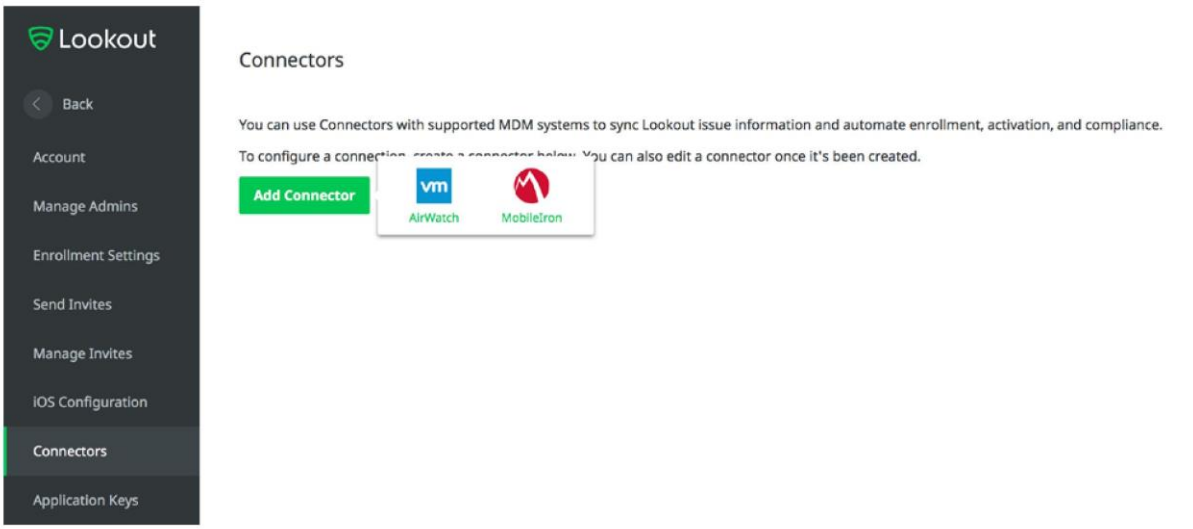


Rysunek 2-117 Konfiguracja aplikacji Lookout z etykietami

2.7.6. DODAWANIE ŁĄCZNIKA MDM DLA SYSTEMU MOBILEIRON DO USŁUGI LOOKOUT MES

Poniższe instrukcje umożliwiają połączenie usługi Lookout z instancją systemu MobileIron i powiązanie stanów urządzeń Lookout z utworzonymi wcześniej etykietami MobileIron.

1. Korzystając z najnowszej wersji dozwolonych adresów IP usługi MDM dostępnej w portalu pomocy technicznej Lookout, skonfiguruj zapory sieciowe organizacji, aby zezwalały na połączenia przychodzące z adresów IP podanych dla portu 443 do instancji MobileIron Core.
2. W portalu Lookout MES przejdź do części Lookout > System > Connectors (Łączniki).
3. Na stronie **Connectors** (Łączniki):
    a. Wybierz opcje **Add Connector** (Dodaj łącznik) > **MobileIron**. Zostanie otwarty nowy formularz.



Rysunek 2-118 Ekran dodawania łącznika do usługi Lookout

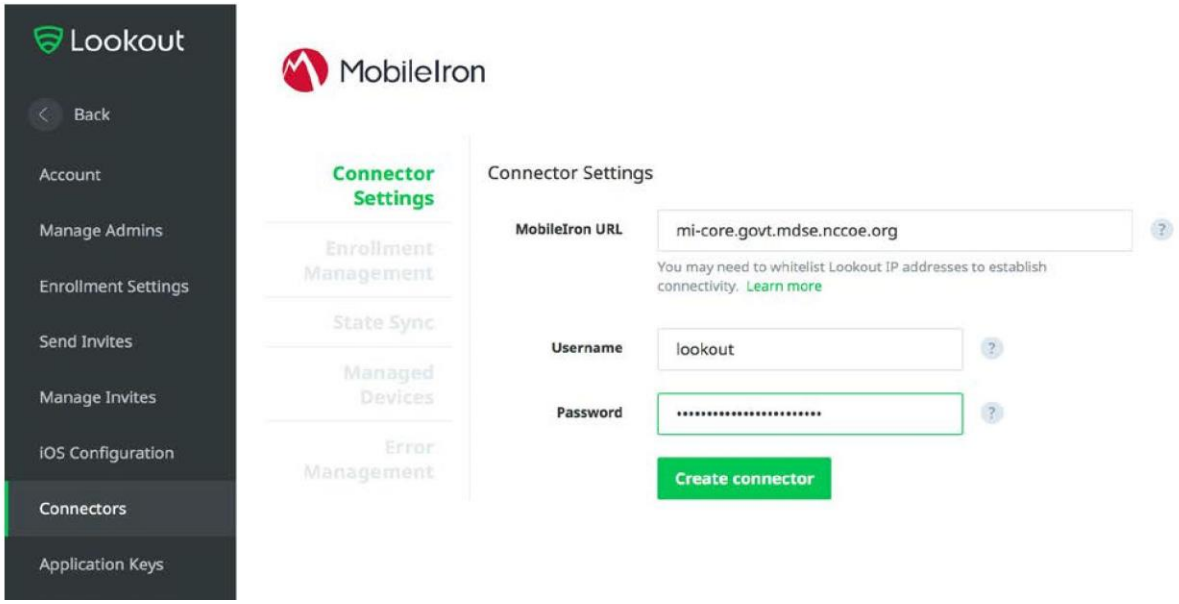
b. W części **Connector Settings** (Ustawienia łącznika) formularza:

   i. W polu **MobileIron URL** (Adres URL MobileIron) wprowadź nazwę FQDN instancji systemu MobileIron. W naszym przykładowym wdrożeniu adres URL to **mi-core.govt.mdse.nccoe.org**.

   ii. W polu **Username** (Nazwa użytkownika) wprowadź identyfikator użytkownika konta administratora systemu MobileIron utworzonego w punkcie 2.7.1. W naszym przykładowym wdrożeniu nazwa wprowadzona w polu **User ID** (Identyfikator użytkownika) to **lookout**.

   iii. W polu **Password** (Hasło) wprowadź hasło powiązane z danym kontem administratora systemu MobileIron.

   iv. Kliknij przycisk **Create Connector** (Utwórz łącznik). Spowoduje to wyświetlenie dodatkowych części formularza.



Rysunek 2-119 Ustawienia łącznika

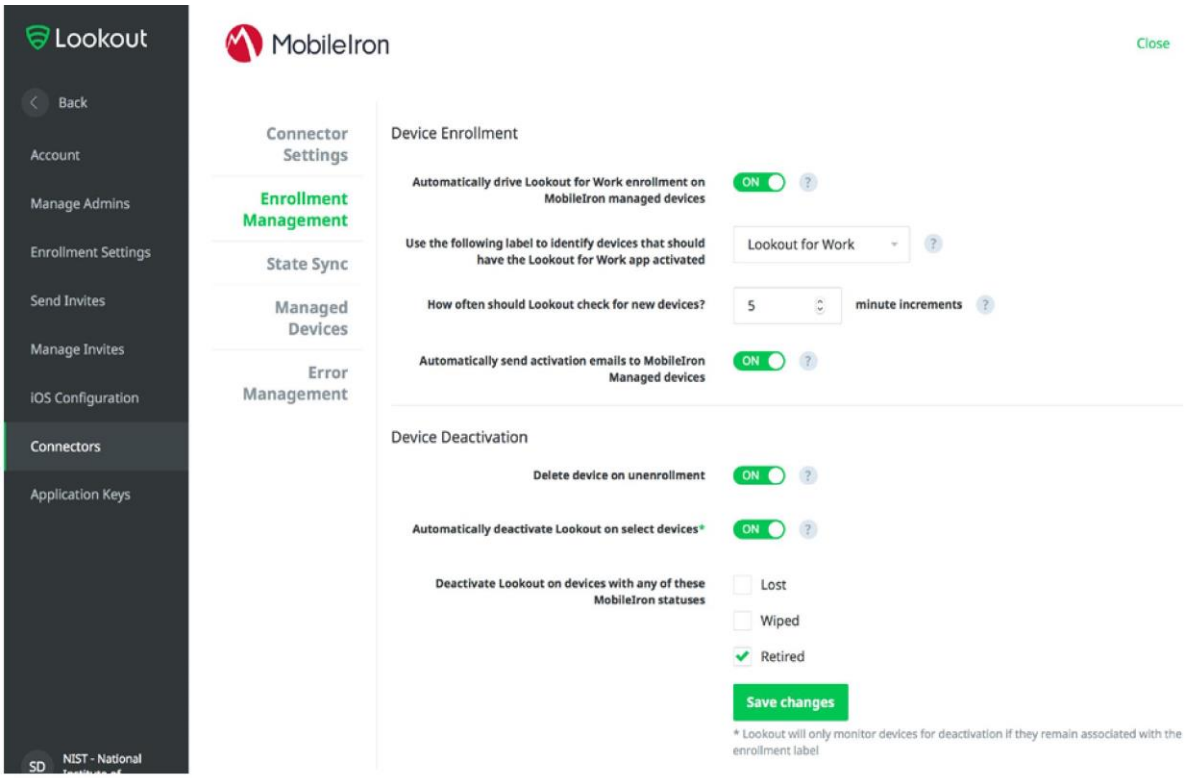
c. W obszarze **Enrollment Management** (Zarządzanie rejestracją) formularza:

   i. Wybierz opcję **ON** (WŁ.) dla przełącznika **Device Enrollment** (Rejestracja urządzeń) > **Automatically drive Lookout for Work enrollment on MobileIron managed devices** (Automatycznie przeprowadź rejestrację aplikacji Lookout for Work na urządzeniach zarządzanych przez system MobileIron).

   ii. Z rozwijanego menu **Device Enrollment** (Rejestracja urządzeń) > **Use the following label to identify devices that should have the Lookout for Work app activated** (Użyj następującej etykiety do identyfikacji urządzeń, na których powinna być aktywowana aplikacja Lookout for Work) wybierz etykietę Lookout for Work.

   iii. Wybierz opcję **ON** (WŁ.) dla przełącznika **Device Enrollment** (Rejestracja urządzeń) > **Automatically send activation emails to MobileIron managed devices** (Automatycznie wysyłaj aktywacyjne wiadomości e-mail do urządzeń zarządzanych przez system MobileIron).

   iv. Kliknij przycisk **Save Changes** (Zapisz zmiany).



Rysunek 2-120 Ustawienia rejestracji łącznika

d. W części **State Sync** (Synchronizacja stanu) formularza:

   i. Wybierz opcję **ON** (WŁ.) dla przełącznika **State Sync** (Synchronizacja stanu) > **Synchronize Device Status to MobileIron** (Synchronizuj stan urządzenia z systemem MobileIron).

   ii. Dla każdego punktu w poniższej tabeli:

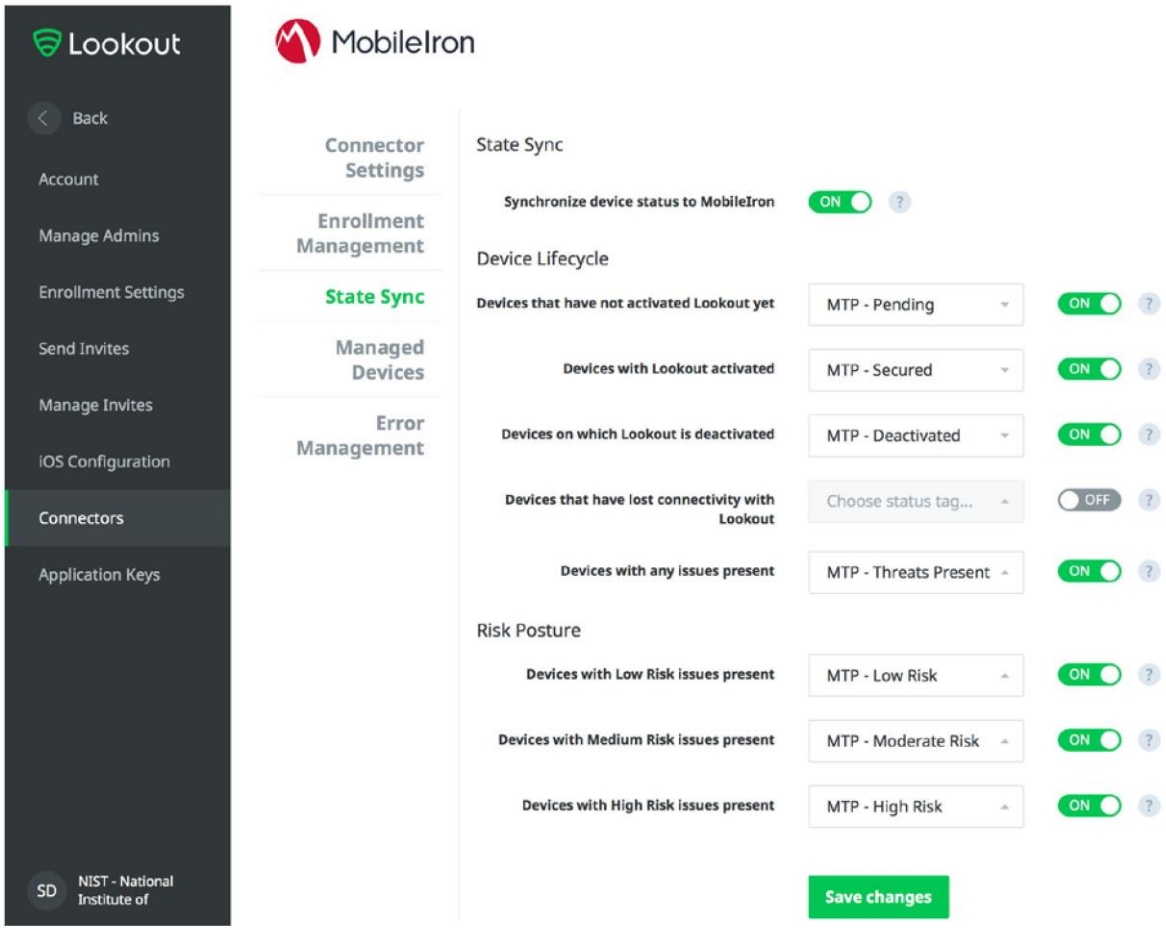
      1) Wybierz opcję **ON** (WŁ.) dla przełącznika.

      2) Z menu rozwijanego wybierz **etykietę MobileIron** z powiązanym celem z tabeli w **punkcie 2.6.2 „Dodawanie etykiet w systemie MobileIron dla usługi Lookout”**. Oto nazwy etykiet, których użyliśmy dla każdego celu w naszym przykładowym wdrożeniu.

Stan	Cel	Nazwa etykiety
Urządzenia, na których nie aktywowano jeszcze usługi Lookout.	Zarządzanie cyklem życia: urządzenia, na których usługa Lookout nie została jeszcze aktywowana.	MTP Pending (MTP — oczekujące)
Urządzenia z aktywowaną usługą Lookout.	Zarządzanie cyklem życia: urządzenia, na których usługa Lookout została aktywowana.	MTP Secured (MTP — zabezpieczone)
Urządzenia, na których usługa Lookout jest dezaktywowana.	Zarządzanie cyklem życia: urządzenia, na których usługa Lookout została dezaktywowana.	MTP Deactivated (MTP — dezaktywowano)
Urządzenia, z którymi obecnie występują problemy.	Zarządzanie cyklem życia: urządzenia z zagrożeniami wykrytymi przez usługę Lookout.	MTP Threats Detected (MTP — wykryto zagrożenia)
Urządzenia z obecnymi problemami niskiego ryzyka.	Poziom ryzyka: urządzenia o niskiej ocenie ryzyka w usłudze Lookout.	MTP Low Risk (MTP— niskie ryzyko)
Urządzenia z którymi obecnie jest związane umiarkowane ryzyko.	Poziom ryzyka: urządzenia o umiarkowanej ocenie ryzyka w usłudze Lookout.	MTP Moderate Risk (MTP— umiarkowane ryzyko)
Urządzenia z którymi obecnie jest związane wysokie ryzyko.	Poziom ryzyka: urządzenia o wysokiej ocenie ryzyka w usłudze Lookout.	MTP High Risk (MTP— wysokie ryzyko)

Uwaga: Administratorzy mogą zmieniać nazwy etykiet na bardziej odpowiednie dla ich środowiska.

iii. Kliknij przycisk **Save Changes** (Zapisz zmiany).



Rysunek 2-121 Ustawienia synchronizacji łącznika

2.7.7. KONFIGUROWANIE REAKCJI SYSTEMU MOBILEIRON NA RYZYKO

Wykonanie poniższych kroków umożliwi systemowi MobileIron generowanie odpowiedzi na różne stany urządzeń przypisane do nich przez usługę Lookout, np. MTP High Risk (MTP — wysokie ryzyko).

2.7.7.1. DODAWANIE REGUŁY KONTROLI APLIKACJI W SYSTEMIE MOBILEIRON

1. Na stronie **MobileIron Admin Portal** przejdź do części **Apps** (Aplikacje) > **App Control** (Kontrola aplikacji).
2. Kliknij przycisk **Add** (Dodaj). Zostanie wyświetlone okno dialogowe **Add App Control Rule** (Dodaj regułę kontroli aplikacji).
3. W oknie dialogowym **Add App Control Rule** (Dodaj regułę kontroli aplikacji):

a. W polu **Name** (Nazwa) wpisz **Threats Present Trigger** (Wyzwalacz obecnych zagrożeń).

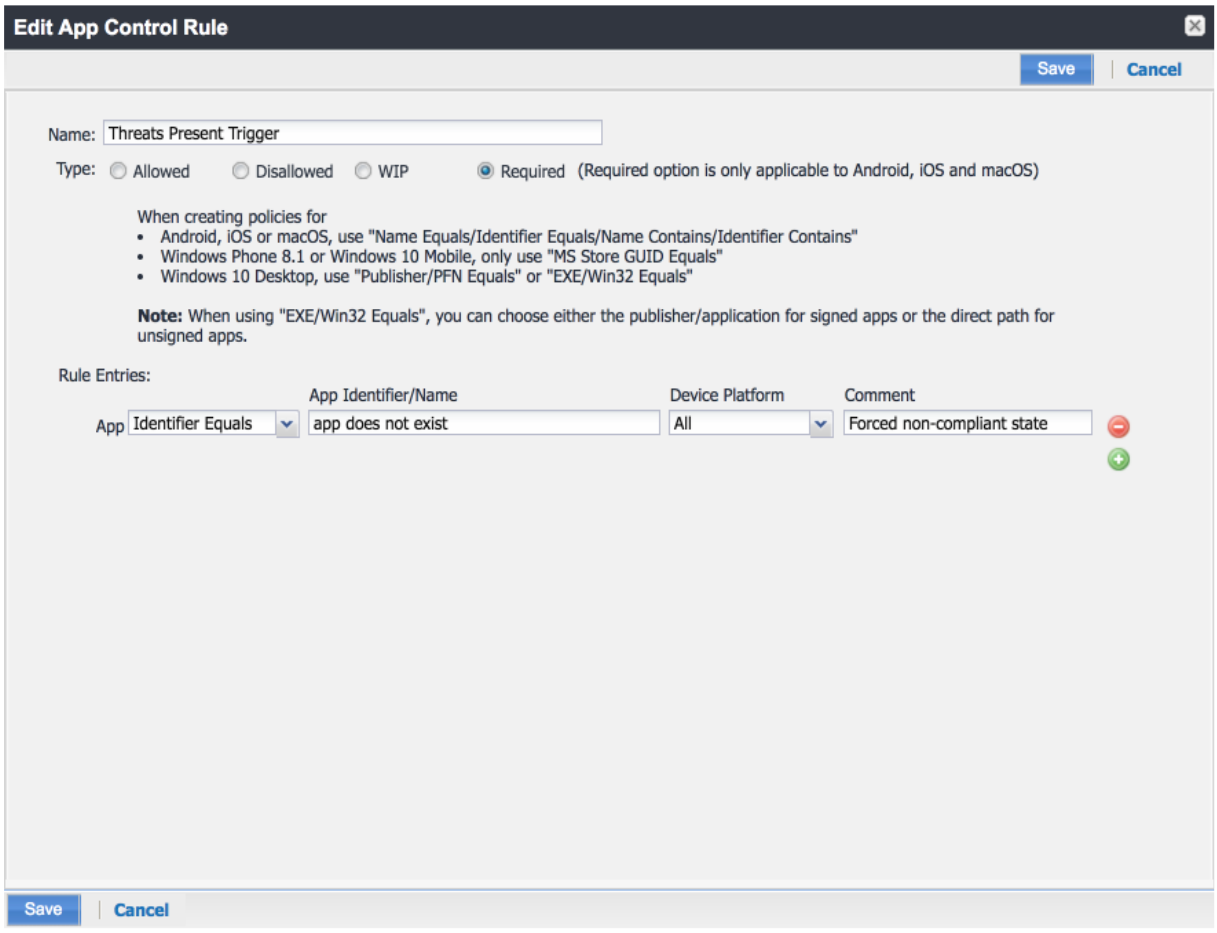
b. Dla ustawienia **Type** (Typ) wybierz opcję **Required** (Wymagana).

c. W polu **App Identifier/Name** (Identyfikator/nazwa aplikacji) wpisz **app does not exist** (aplikacja nie istnieje).

d. Z menu rozwijanego **Device Platform** (Platforma urządzenia) wybierz opcję **All** (Wszystkie).

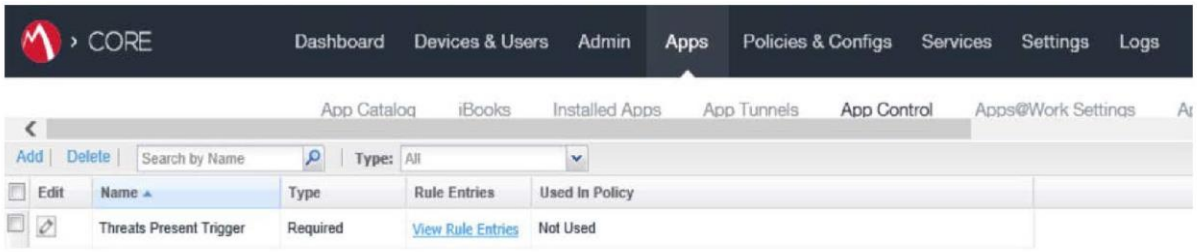
e. W polu **Comment** (Komentarz) opcjonalnie wpisz **Forces non-compliant state** (Wymusza stan niezgodności).

f. Kliknij przycisk **Save** (Zapisz).



Rysunek 2-122 Reguła kontroli aplikacji w systemie MobileIron

4. Nowa reguła kontroli aplikacji powinna teraz pojawić się na stronie **Apps** (Aplikacje) > **App Control** (Kontrola aplikacji).



Rysunek 2-123 Reguła kontroli aplikacji w systemie MobileIron

2.7.7.2. DODAWANIE AKCJI ZGODNOŚCI W SYSTEMIE MOBILEIRON

Akcja **Compliance** (Zgodność) określa, jakie działania podejmie system MobileIron, gdy zasada **App Control** (Kontrola aplikacji), taka jak ta utworzona w poprzednim punkcie, zostanie naruszona przez zarządzane urządzenie mobilne. Poniższe kroki umożliwiają utworzenie i skonfigurowanie przykładowej akcji zgodności w odpowiedzi na naruszenie reguły kontroli aplikacji **MTP High Risk** (MTP — wysokie ryzyko). Należy pamiętać, że pojedyncza akcja zgodności może być powiązana z wieloma regułami kontroli aplikacji, jeśli dla każdej z nich zostanie skonfigurowana ta sama odpowiedź. W przeciwnym razie należy utworzyć nową akcję zgodności.

1. Na stronie **MobileIron Admin Portal** przejdź do części **Policies & Configs** (Zasady i konfiguracja) > **Compliance Actions** (Akcje zgodności).
2. Kliknij przycisk **Add** (Dodaj). Zostanie otwarte okno dialogowe **Add Compliance Action** (Dodaj akcję zgodności).
3. W oknie dialogowym **Add Compliance Action** (Dodaj akcję zgodności):
    a. W polu **Name** (Nazwa) dodaj opis akcji zgodności. Zalecamy określenie rodzaju podejmowanego działania. W tym przykładzie zilustrowano tworzenie akcji zgodności, która będzie powiązana z etykietą **MTP High Risk** (MTP — wysokie ryzyko).
    b. Zaznacz pole wyboru **Enforce Compliance Actions Locally on Devices** (Wymuszaj akcje zgodności lokalnie na urządzeniach).

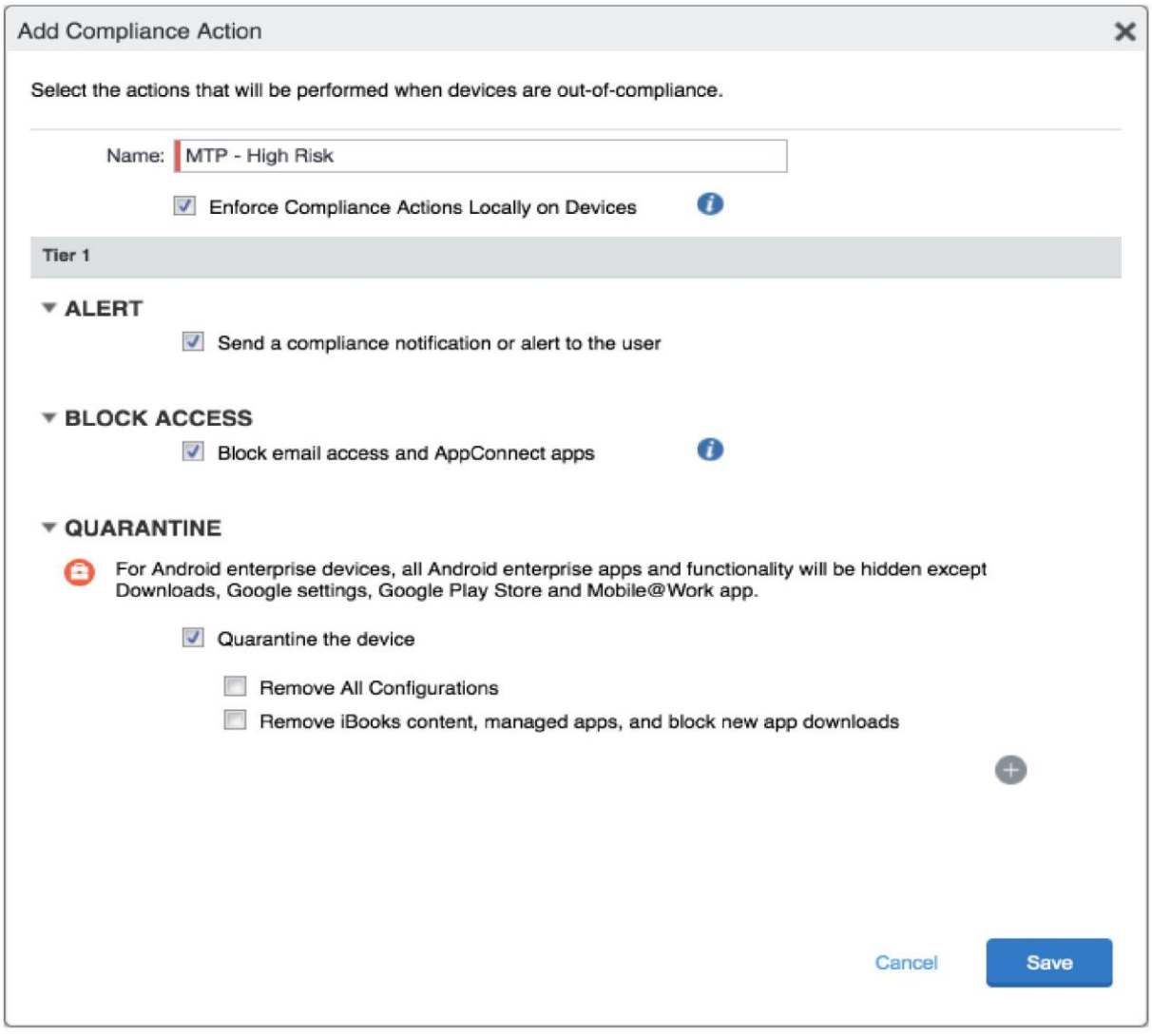
c. Zaznacz pole wyboru **Send a compliance notification or alert to the user** (Wyślij powiadomienie o zgodności lub alert do użytkownika).

d. Zaznacz pole wyboru **Block email access and AppConnect apps** (Zablokuj dostęp do poczty elektronicznej i aplikacji AppConnect).

e. Zaznacz pole wyboru **Quarantine the device** (Poddaj urządzenie kwarantannie).

f. Usuń zaznaczenie pola wyboru **Remove All Configurations** (Usuń wszystkie konfiguracje).

g. Kliknij przycisk **Save** (Zapisz).

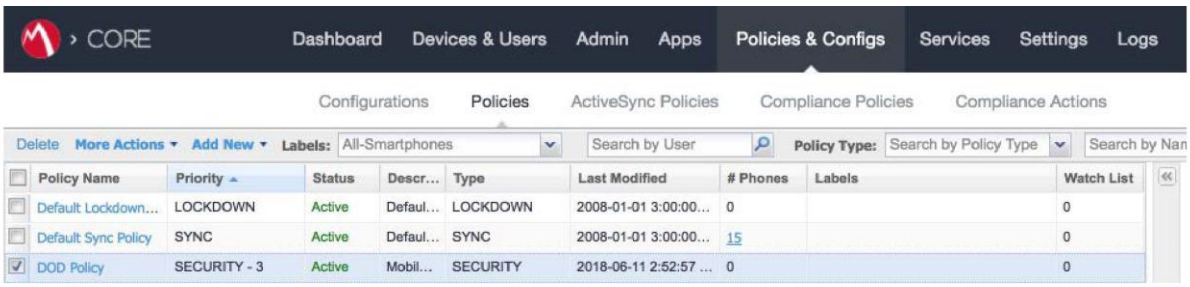


Rysunek 2-124 Akcja zgodności MTP High Risk

2.7.7.3. TWORZENIE ZASADY BEZPIECZEŃSTWA SYSTEMU MOBILEIRON DLA USŁUGI LOOKOUT MES

Oprócz potencjalnego określania innych środków bezpieczeństwa, takich jak: wymagania dotyczące haseł, zasady bezpieczeństwa mogą wiązać akcję zgodności z regułami kontroli aplikacji, umożliwiając systemowi MobileIron wykonywanie skonfigurowanych akcji za każdym razem, gdy urządzenie, dla którego zastosowano te zasady, naruszy regułę kontroli aplikacji. Poniższe kroki umożliwiają utworzenie nowej zasady bezpieczeństwa dla urządzeń o stanie **MES High Risk** stwierdzonym przez usługę Lookout, przy użyciu istniejącej zasady jako punktu odniesienia, na podstawie którego można zastosować bardziej rygorystyczne mechanizmy kontroli.

1. Na stronie **MobileIron Admin Portal** przejdź do części **Policies & Configs** (Zasady i konfiguracja) > **Policies** (Zasady).
2. Na stronie **Policies** (Zasady):
    a. Wybierz zasadę bezpieczeństwa, która ma być wykorzystana jako punkt odniesienia.
    b. Kliknij kolejno opcje **More Actions** (Więcej akcji) > **Save As** (Zapisz jako). Spowoduje to otwarcie okna dialogowego **New Security Policy** (Nowa zasada bezpieczeństwa).



Rysunek 2-125 Wybór zasady odniesienia

    c. W oknie dialogowym **New Security Policy** (Nowa zasada bezpieczeństwa):
        i. W polu **Name** (Nazwa) zmień nazwę zasady na **MTP High Risk** (MTP — wysokie ryzyko).

ii. Z menu rozwijanego **Priority** (Priorytet) wybierz aktualną zasadę. W oparciu o ten wybór nowa zasada będzie traktowana priorytetowo. W tym przykładzie nowa zasada jest wyżej w hierarchii niż **MTP Medium Risk** (MTP — umiarkowane ryzyko). **Uwaga**: Aby ułatwić ustawianie priorytetów, zaleca się dodawanie nowych zasad bezpieczeństwa w kolejności rosnącej (od najniższego do najwyższego priorytetu).

Rysunek 2-126 Akcja zgodności MTP High Risk (MTP — wysokie ryzyko)

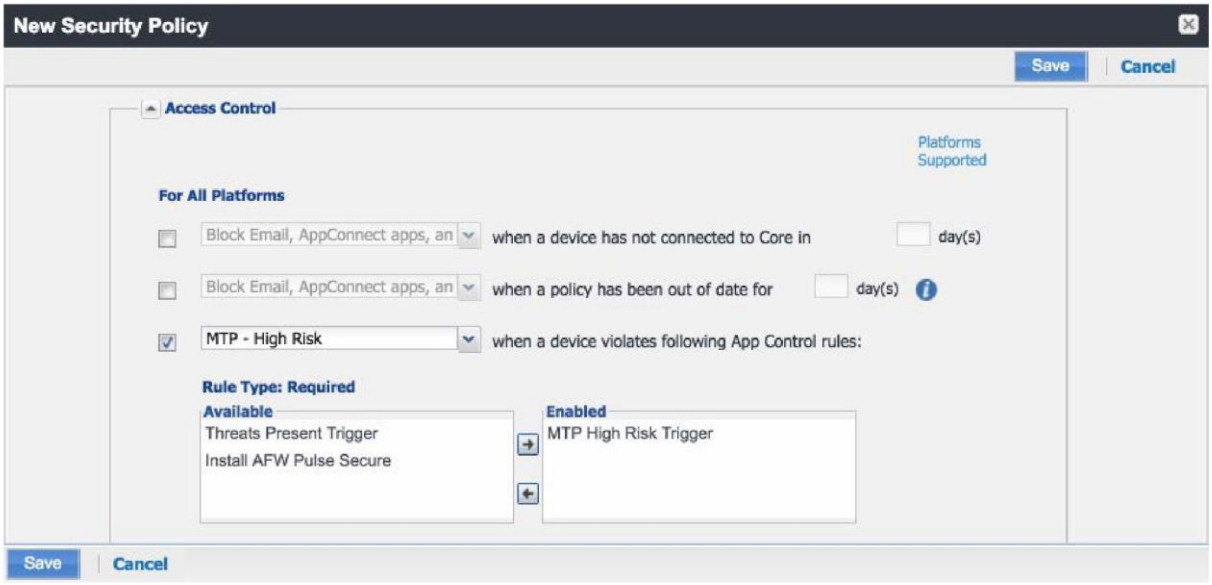
iii. W części **Access Control** (Kontrola dostępu) > **For All Platforms** (Dla wszystkich platform):

1) Z menu rozwijanego **when a device violates the following app control rules** (gdy urządzenie narusza następujące reguły kontroli aplikacji) wybierz akcję zgodności MTP - High Risk (MTP - wysokie ryzyko).

2) Z listy reguł kontroli aplikacji **Available** (Dostępne) wybierz pozycję **MTP - High Risk Trigger** (Wyzwalacz MTP - wysokie ryzyko).

3) Kliknij **strzałkę w prawo**, aby przenieść pozycję MTP High Risk Trigger (Wyzwalacz MTP - wysokie ryzyko) na listę **Enabled** (Włączone).

iv. Kliknij przycisk **Save** (Zapisz).



Rysunek 2-127 Wyzwalacz zasady bezpieczeństwa

2.7.7.4. ZASTOSOWANIE ETYKIETY USŁUGI LOOKOUT MES DO ZASADY BEZPIECZEŃSTWA SYSTEMU MOBILEIRON

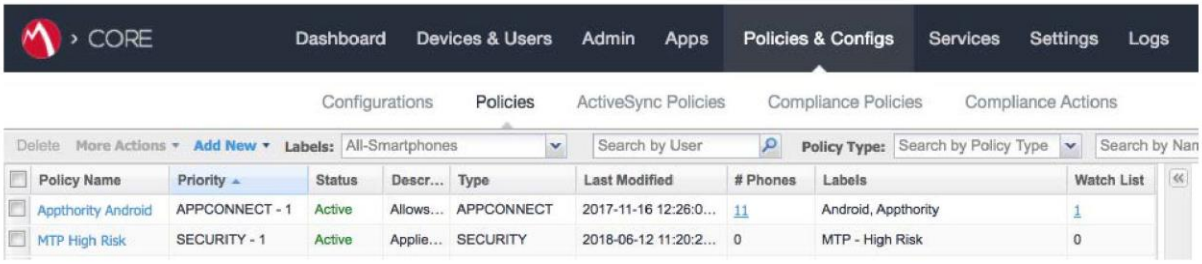
Poniższe kroki umożliwiają zastosowanie etykiety MTP - High Risk (MTP - wysokie ryzyko) do zasady bezpieczeństwa utworzonej w poprzednim punkcie. Dzięki temu, gdy usługa w chmurze Lookout zastosuje etykietę do dowolnego urządzenia z wykrytym zagrożeniem wysokiego ryzyka i takie urządzenie zostanie zarejestrowane w systemie MobileIron, zasada bezpieczeństwa zostanie dla niego automatycznie zastosowana (pod warunkiem, że ma wyższy priorytet niż aktualnie stosowana zasada). To z kolei spowoduje naruszenie zasady kontroli aplikacji z wyzwalaczem MTP - High Risk i podjęcie akcji zgodności MTP - High Risk. Gdy usługa Lookout wykryje, że zagrożenie zostało wyeliminowane, usunie etykietę MTP - High Risk, a podczas rejestracji urządzenia w systemie MobileIron zostanie zastosowana kolejna zasada bezpieczeństwa o niższym priorytecie.

1. Na stronie **MobileIron Admin Portal** przejdź do części **Policies & Configs** (Zasady i konfiguracja) > **Policies** (Zasady).

2. Na stronie **Policies** (Zasady):

a. Zaznacz pole wyboru zasady bezpieczeństwa **MTP - High Risk** (MTP - wysokie ryzyko).

b. Wybierz opcje **More Actions** (Więcej akcji) > **Apply To Label** (Zastosuj do etykiety). Zostanie wyświetlone okno dialogowe Apply To Label (Zastosuj do etykiety).

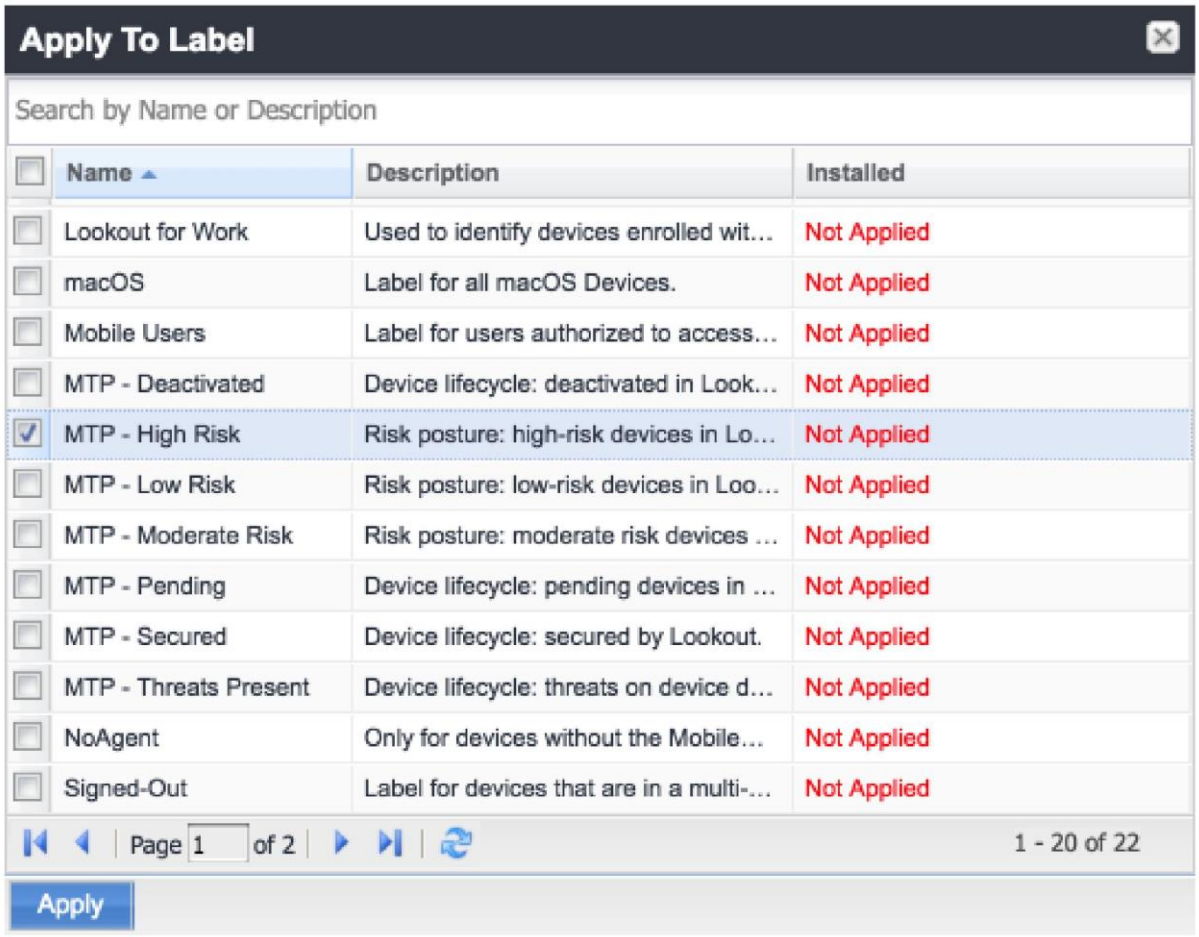


Rysunek 2-128 Lista zasad

c. W oknie dialogowym **Apply To Label** (Zastosuj do etykiety):

i. Zaznacz pole wyboru etykiety **MTP - High Risk** (MTP - wysokie ryzyko).

ii. Kliknij przycisk **Apply** (Zastosuj).



Rysunek 2-129 Okno dialogowe Apply To Label (Zastosuj do etykiety)

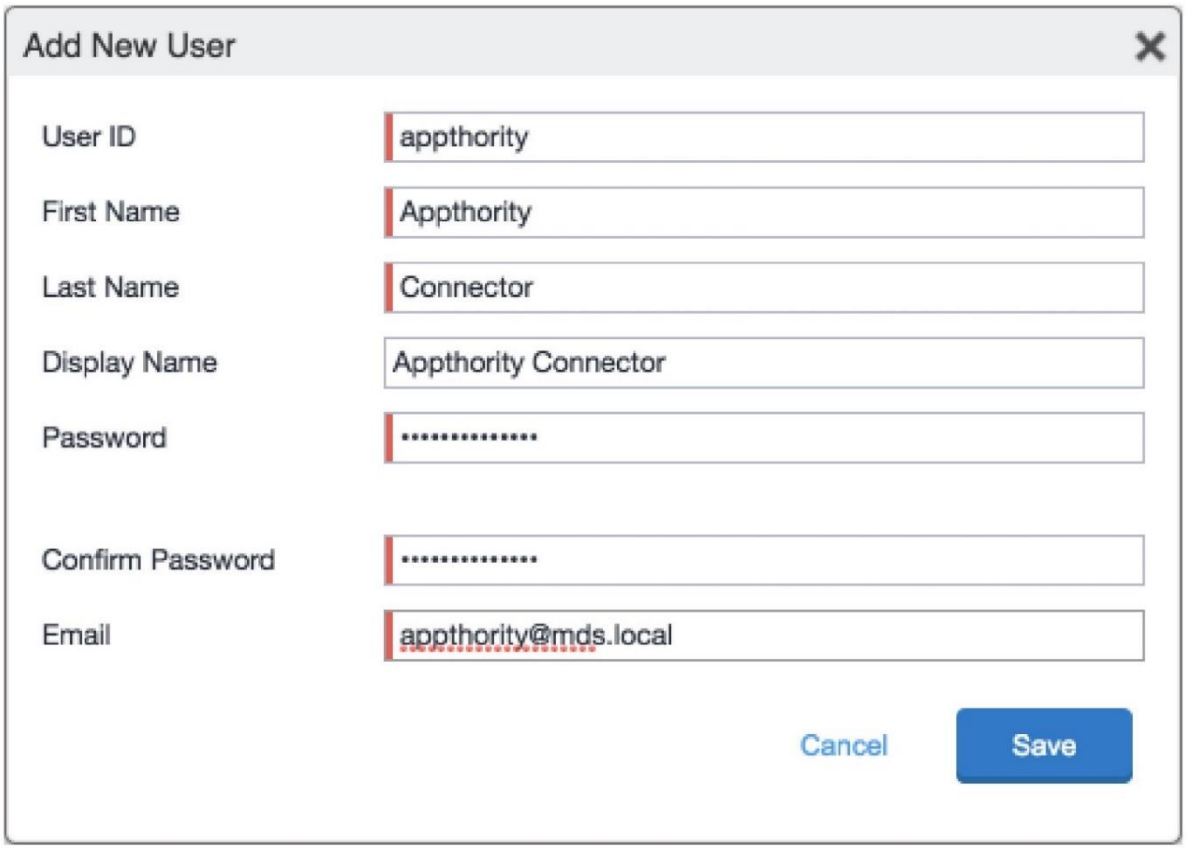
2.8. INTEGRACJA USŁUGI APPTHORITY MOBILE THREAT DETECTION Z SYSTEMEM MOBILEIRON

Appthority zapewnia lokalny łącznik dla systemu MobileIron, który działa jako kontener Docker w systemie RedHat Linux. Łącznik wykorzystuje interfejs API systemu MobileIron do uzyskiwania informacji o zarządzanych urządzeniach i zainstalowanych na nich aplikacjach, które są następnie synchronizowane z instancją usługi w chmurze w celu uzyskania ocen ryzyka dla aplikacji i urządzeń, które są przypisywane do urządzeń przy użyciu niestandardowych atrybutów. W poniższych punktach przedstawiono kroki, które należy wykonać, aby utworzyć konto API w systemie MobileIron oraz wdrożyć i skonfigurować łącznik Appthority.

2.8.1. TWORZENIE KONTA API W SYSTEMIE MOBILEIRON DLA ŁĄCZNIKA APPTHORITY

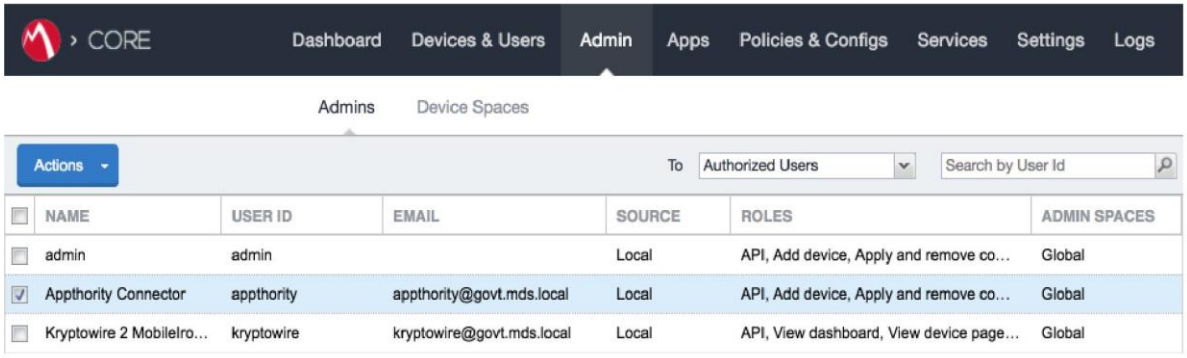
Poniższe kroki umożliwią utworzenie konta administracyjnego, które nada usłudze Appthority określone uprawnienia wymagane w systemie MobileIron.

1. Na stronie **MobileIron Admin Portal** przejdź do części **Devices & Users** (Urządzenia i użytkownicy) > **Users** (Użytkownicy).
2. Na stronie **Users** (Użytkownicy):
    a. Wybierz opcje **Add** (Dodaj) > **Add Local User** (Dodaj użytkownika lokalnego). Zostanie otwarte okno dialogowe **Add New User** (Dodaj nowego użytkownika).
    b. W oknie dialogowym **Add New User** (Dodaj nowego użytkownika):
        i. W polu **User ID** (Identyfikator użytkownika) wprowadź **tożsamość użytkownika**, przy użyciu której będzie uwierzytelniany łącznik Appthority. W naszym wdrożeniu użyto nazwy **Appthority**.
        ii. W polu **First Name** (Imię) wprowadź ogólne imię dla usługi **Appthority**.
        iii. W polu **Last Name** (Nazwisko) wprowadź ogólne nazwisko dla usługi **Appthority**.
        iv. W polu **Display Name** (Wyświetlana nazwa) można opcjonalnie wprowadzić wyświetlaną nazwę dla tego konta użytkownika.
        v. W polu **Password** (Hasło) podaj hasło, którego tożsamość **Appthority** będzie używać do uwierzytelniania w systemie MobileIron.
        vi. W polu **Confirm Password** (Potwierdź hasło) wprowadź to samo hasło, co w poprzednim kroku.
        vii. W polu **Email** należy podaj konto e-mail dla tożsamości **Appthority**. Powinno to być konto kontrolowane przez organizację.
        viii. Kliknij przycisk **Save** (Zapisz).



Rysunek 2-130 Ustawienia użytkownika dla usługi Appthority

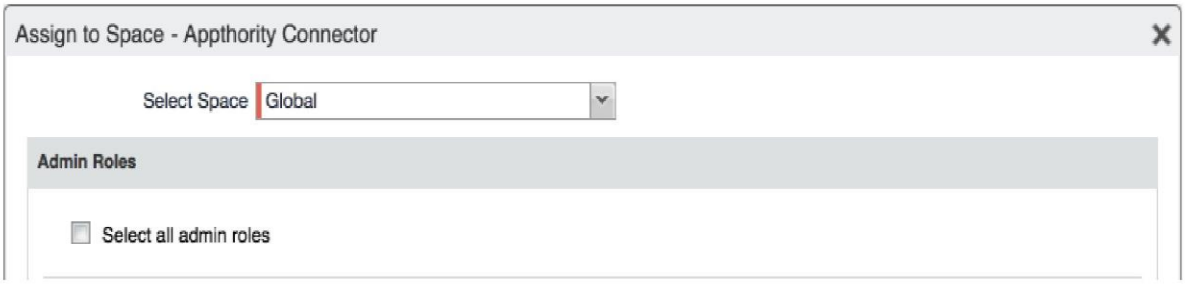
3. Na stronie **MobileIron Admin Portal** przejdź do części **Admin** (Administrator).
4. Na stronie **Admin** (Administrator):
    a. Zaznacz pole wyboru konta utworzonego dla usługi **Appthority** w kroku 2.
    b. Wybierz opcję **Actions** (Akcje) > **Assign to Space** (Przypisz do przestrzeni). Spowoduje to otwarcie okna dialogowego **Assign to Space** (Przypisz do przestrzeni) dla konta **Appthority**.



Rysunek 2-131 Użytkownik dla łącznika usługi Appthority

c. W oknie dialogowym **Assign to Space** (Przypisz do przestrzeni):

i. Z menu rozwijanego **Select Space** (Wybierz przestrzeń) wybierz opcję **Global** (Globalna).



Rysunek 2-132 Przypisywanie przestrzeni do łącznika usługi Appthority

ii. **Włącz** każde z ustawień wymienionych poniżej:

Device Management (Zarządzanie urządzeniami) > View device page, device details (Wyświetl stronę urządzenia, szczegóły urządzenia)
Privacy Control (Kontrola prywatności) > View apps and ibooks in device details (Wyświetl aplikacje i pliki iBook w szczegółach urządzenia)
App Management (Zarządzanie aplikacjami) > Apply and remove application label (Zastosuj i usuń etykietę aplikacji)
Other Roles (Inne role) > API

iii. Kliknij przycisk **Save** (Zapisz).

2.8.2. WDROŻENIE APPTHORITY CONNECTOR OPEN VIRTUALIZATION APPLIANCE

Jedną z opcji wdrożenia łącznika usługi Appthority jest wstępnie skonfigurowana maszyna wirtualna RedHat dystrybuowana jako otwarte urządzenie wirtualizacyjne (*ang. Open Virtualization Appliance – OVA*). Urządzenie OVA zostało zaimportowane do naszego wirtualnego środowiska laboratoryjnego zgodnie z instrukcjami zawartymi w dokumencie *Connector On-Premises: Virtual Machine Setup* dostępnej na portalu pomocy technicznej usługi Appthority pod adresem: https://support.appthority.com/.

2.8.3. URUCHOMIENIE SKRYPTU DO WDRAŻANIA ŁĄCZNIKA DLA SYSTEMU ZARZĄDZANIA MOBILNOŚCIĄ W PRZEDSIĘBIORSTWIE

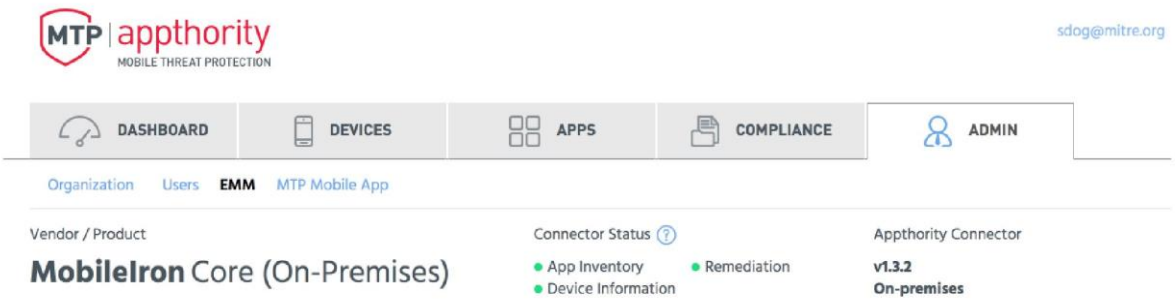
Po uruchomieniu kontenera Docker usługi Appthority, skrypt instalacyjny skonfiguruje go do korzystania z utworzonego wcześniej konta API w systemie MobileIron. Szczegółowe instrukcje dotyczące korzystania ze skryptu są dostępne w portalu pomocy technicznej usługi Appthority pod adresem: https://help-mtp.appthority.com/SetUp/EMM/EMM Script/Run-EMMDeployScript.html. Pierwsze dwa kroki wymagają podania danych uwierzytelniających dostarczonych przez Appthority, niezbędnych do zweryfikowania subskrypcji i powiązania łącznika z właściwą instancją usługi w chmurze. W trzecim kroku należy podać szczegółowe informacje umożliwiające integrację z lokalną instancją systemu MobileIron Core. Uzyskane przez nas wyniki po wykonaniu trzeciego kroku przedstawiono poniżej.

1. **Pobierz** kopię dokumentu *Run the EMM Connector Deployment Script* z portalu pomocy technicznej Appthority, która jest dostępna pod adresem: https://help-mtp.appthority.com/SetUp/EMM/EMM Script/Run- EMMDeployScript.html (konieczne jest uwierzytelnienie w portalu).
2. **Uruchom** skrypt. Trzeci krok w skrypcie wymaga podania ustawień umożliwiających łącznikowi Appthority komunikację z systemem MobileIron Core. Wyniki wykonania tego kroku przedstawiono poniżej dla celów informacyjnych.

```
Selection: 3

Configure EMM
-------------------------------------
Select EMM Provider:

[A]  - AirWatch 9.X
[M]  - MobileIron Core 9.X
[MC] - MobileIron Cloud

EMM Provider:           M
EMM Provider Selected:  mobileiron
Is MobileIron Core On-Premise? (y/n): y
EMM URL:                mi-core.govt.mdse.nccoe.org
Is the EMM User a Domain Account (y/n)? n
EMM Username:           appthority
EMM Password:
Is there a Proxy (y/n)? n
Set EMM API Timeout (y/n)? n

[Okay]
```

Rysunek 2-133 Konfiguracja łącznika usługi Appthority w interfejsie wiersza polecenia (*ang. Command Line Interface – CLI*)

3. Po wykonaniu skryptu sprawdź pomyślną synchronizację z usługą Appthority w chmurze, wchodząc do portalu Appthority MTP, klikając opcje **Admin** (Administrator) > **EMM** i przeglądając elementy w obszarze **Connector Status** (Status łącznika).



Rysunek 2-134 Status łącznika usługi Appthority EMM

2.9. REJESTROWANIE URZĄDZEŃ W SYSTEMIE MOBILEIRON CORE

W tym scenariuszu pracownik zarządza swoimi osobistymi aplikacjami, danymi i wieloma funkcjami urządzenia. Organizacja zarządza aplikacjami i danymi związanymi z pracą oraz ma kontrolę nad określonymi funkcjami urządzenia, takimi jak wymaganie złożonego

kodu PIN odblokowującego urządzenie lub możliwość zdalnego wymazania pamięci zgubionego urządzenia. Mechanizmy umożliwiające osiągnięcie podobnej charakterystyki bezpieczeństwa różnią się między urządzeniami z systemem iOS i Android.

2.9.1. NADZOROWANIE I REJESTROWANIE URZĄDZEŃ Z SYSTEMEM IOS

Wiele środków bezpieczeństwa opartych na systemie MDM można stosować tylko na urządzeniach z systemem iOS działających w trybie nadzorowanym. W poniższych krokach opisano, jak włączyć ten tryb na urządzeniu z systemem iOS, a następnie zarejestrować je w systemie MobileIron Core.

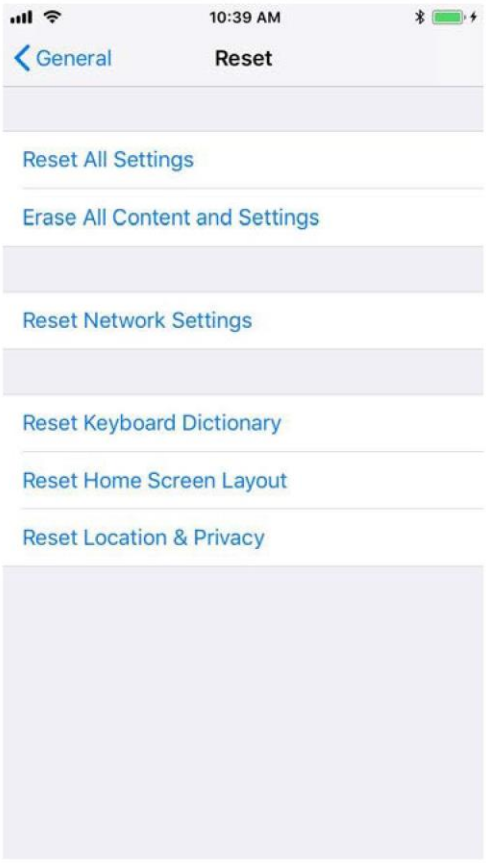
2.9.1.1. RESETOWANIE URZĄDZENIA Z SYSTEMEM IOS

Zanim urządzenie będzie mogło zostać przełączone w tryb nadzorowany, musi znajdować się w stanie po przywróceniu ustawień fabrycznych i mieć usuniętą blokadę aktywacji. Jeśli blokada aktywacji jest włączona, narzędzie **Configurator 2** nie będzie w stanie przełączyć urządzenia w tryb nadzorowany.

2.9.1.1.1. RESETOWANIE NIENADZOROWANEGO URZĄDZENIA ZA POMOCĄ APLIKACJI SETTINGS

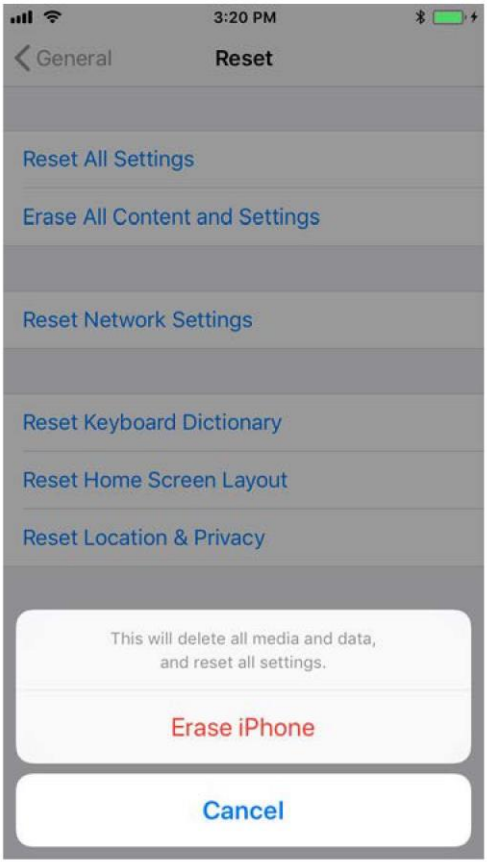
Jeśli urządzenie nie jest jeszcze w trybie nadzorowanym, zaleca się, aby jego aktualny użytkownik ręcznie zresetował i przywrócił ustawienia fabryczne urządzenia, wykonując poniższe czynności:

1. Przejdź do opcji **Settings** (Ustawienia) > **General** (Ogólne) > **Reset**.
2. Wybierz opcję **Erase All Content and Settings** (Wymaż całą zawartość i ustawienia).



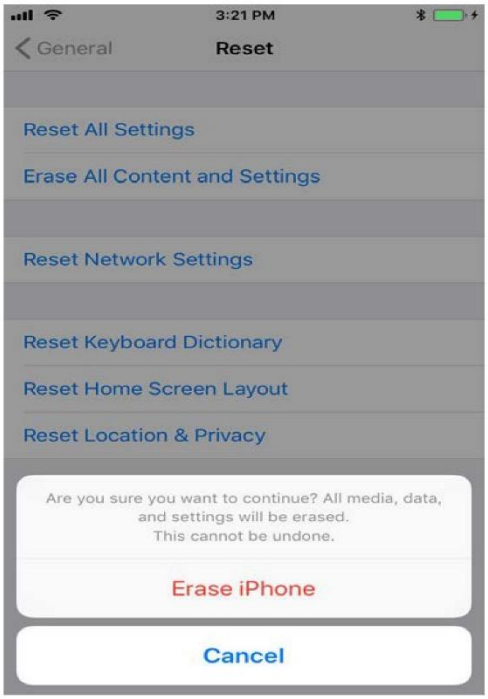
Rysunek 2-135 Ekran resetowania w systemie iOS

3. Po wyświetleniu ostrzeżenia, że spowoduje to usunięcie wszystkich multimediów i danych oraz zresetowanie wszystkich ustawień, wybierz opcję **Erase iPhone** (Wymaż pamięć iPhone'a).



Rysunek 2-136 Potwierdzenie wymazywania pamięci iPhone'a

4. Po wyświetleniu ostrzeżenia, że wszystkie multimedia, dane i ustawienia zostaną nieodwracalnie usunięte, wybierz opcję **Erase iPhone** (Wymaż pamięć iPhone'a). Po zakończeniu procesu resetowania urządzenie uruchomi się ponownie i będzie wymagało aktywacji.



Rysunek 2-137 Ostateczne potwierdzenie wymazywania pamięci iPhone'a

5. Gdy urządzenie wyświetli ekran powitalny, naciśnij przycisk ekranu głównego.
6. Na ekranie **Select Your Language** (Wybierz język) wybierz język **angielski**.
7. Na ekranie **Select Your Country or Region** (Wybierz kraj lub region) wybierz **USA**.
8. Na ekranie **Quick Start** (Szybki start) wybierz opcję **Set up Manually** (Konfiguruj ręcznie).
9. Na ekranie **Choose a Wi-Fi Network** (Wybierz sieć Wi-Fi) wybierz **identyfikator zestawu usług** (*ang. Service Set Identifier – SSID*) dla sieci i uwierzytelnij się w lokalnej sieci Wi-Fi SSID. Urządzenie powinno poinformować użytkownika, że zostało aktywowane. **Uwaga**: Jeśli urządzenie nawiąże połączenie z Internetem z opóźnieniem, konieczna może być ponowna próba aktywacji.
10. **Zatrzymaj się** na ekranie **Data & Privacy** (Dane i prywatność). W tym momencie urządzenie powinno zostać przełączone w **tryb nadzorowany** za pomocą narzędzia **Configurator 2**.

2.9.1.1.2. RESETOWANIE NADZOROWANEGO URZĄDZENIA PRZY UŻYCIU NARZĘDZIA CONFIGURATOR 2

1. Podłącz urządzenie iOS do systemu z uruchomionym narzędziem **Configurator 2** za pośrednictwem **uniwersalnej magistrali szeregowej** (*ang. Universal Serial Bus – USB*).
2. Jeśli urządzenie jest zablokowane, na ekranie **Enter Passcode** (Wprowadź kod dostępu) wprowadź **kod dostępu odblokowujący urządzenie**.

Rysunek 2-138 Wprowadzanie kodu dostępu w systemie iOS

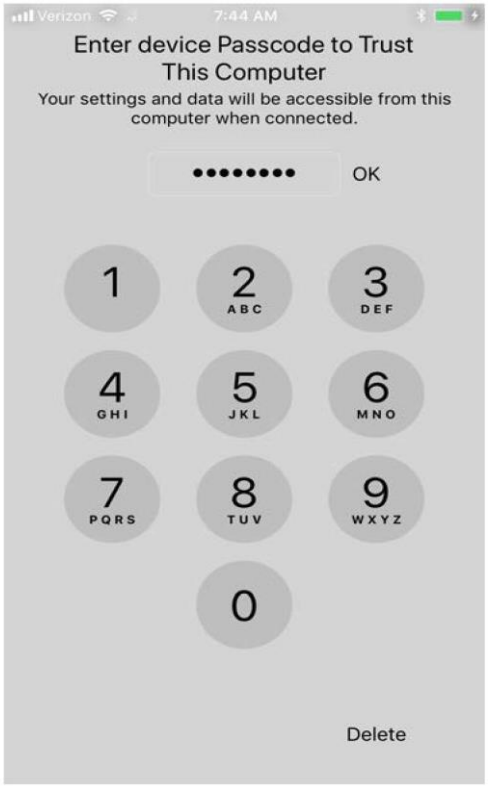
3. W oknie dialogowym **Trust this Computer?** (Zaufać temu komputerowi?) wybierz opcję **Trust** (Zaufaj). Należy pamiętać, że ten krok, wraz z krokiem opisanym poniżej, jest wykonywany tylko przy pierwszym parowaniu urządzenia z danym systemem.

Rysunek 2-139 Potwierdzenie zaufania do komputera w systemie iOS

4. Na ekranie **Enter Device Passcode to Trust This Computer** (Wprowadź kod dostępu do urządzenia, aby zaufać temu komputerowi):

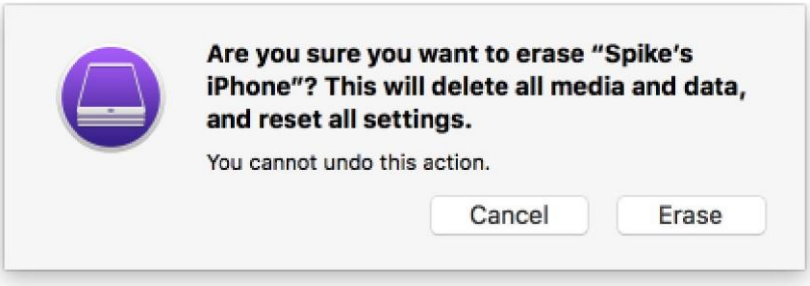
    a. **Wprowadź** kod dostępu odblokowujący urządzenie.

    b. Kliknij przycisk **OK**.



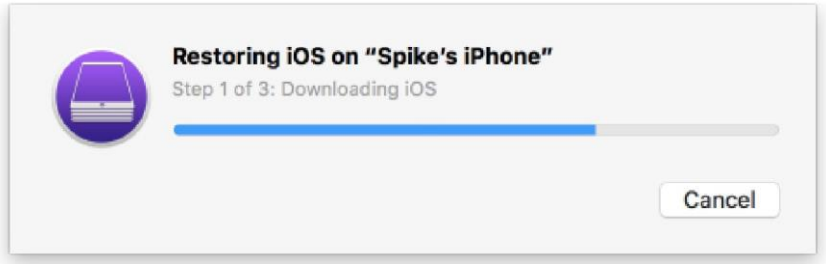
Rysunek 2-140 Wprowadzanie kodu dostępu, aby zaufać komputerowi

5. W narzędziu **Configurator 2** wybierz **symbol** podłączonego urządzenia.
6. Z **menu kontekstowego** wybierz kolejno opcje **Advanced** (Zaawansowane) > **Erase All Content and Settings** (Usuń całą zawartość i ustawienia).
7. W oknie dialogowym **Are you sure you want to erase** (Czy na pewno chcesz wymazać pamięć urządzenia) <nazwa urządzenia>"? wybierz opcję **Erase** (Wymaż).



Rysunek 2-141 Potwierdzenie wymazania pamięci w narzędziu Configurator 2

8. Na ekranie **License Agreement** (Umowa licencyjna):
    a. Przejrzyj umowę licencyjną.
    b. Wybierz opcję **Accept** (Akceptuj), aby zaakceptować licencję i kontynuować korzystanie z oprogramowania.
9. Przywrócenie domyślnych ustawień fabrycznych urządzenia przez narzędzie **Configurator 2** zajmie kilka minut. Narzędzie **Configurator 2** aktywuje także urządzenie po przywróceniu tych ustawień.



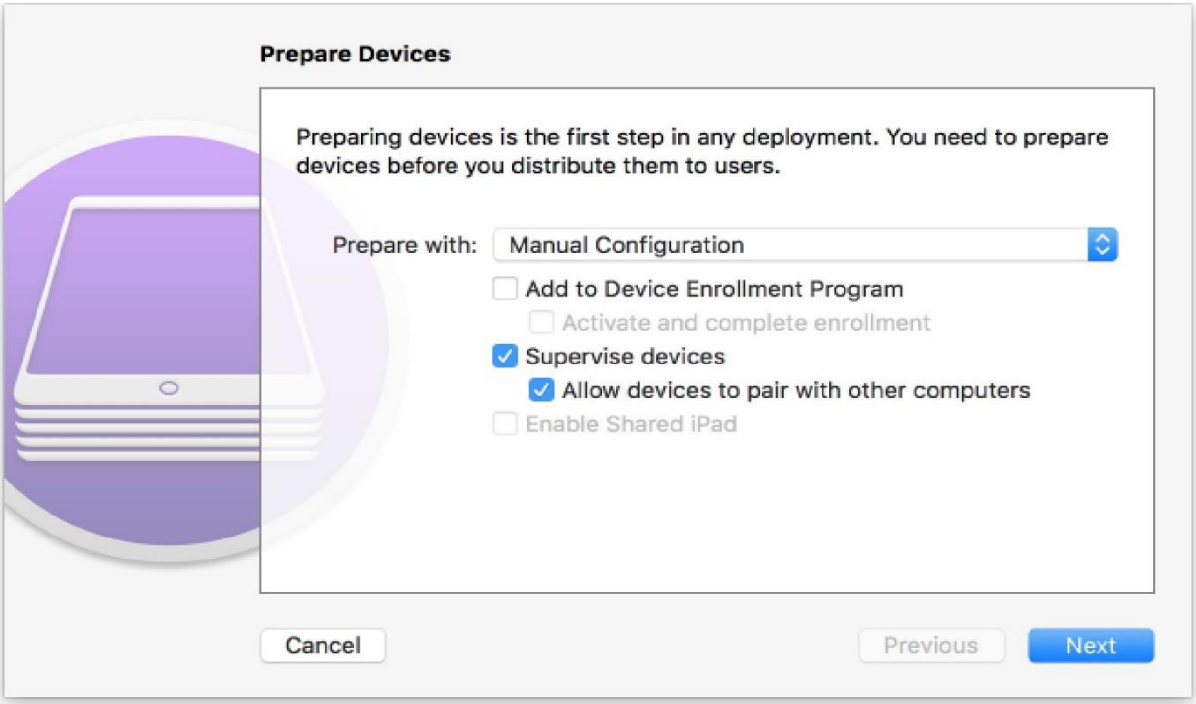
Rysunek 2-142 Przywracanie iPhone'a do ustawień fabrycznych

2.9.1.2. PRZEŁĄCZANIE URZĄDZENIA Z SYSTEMEM IOS W TRYB NADZOROWANY

Urządzenia z systemem iOS, które zostały przywrócone do ustawień fabrycznych, a następnie aktywowane (blokada aktywacji została usunięta), mogą zostać przełączone w tryb nadzorowany za pomocą oprogramowania firmy Apple, Configurator 2, poprzez wykonanie następujących kroków:

1. **Sparuj** docelowe urządzenie iOS z systemem, na którym jest uruchomione narzędzie Configurator 2 przez port USB.
2. Przejdź do ekranu **Configurator 2 > Unsupervised** (Nienadzorowane). Powinien się pojawić symbol podłączonego urządzenia.
3. Na karcie **All Devices** (Wszystkie urządzenia):
    a. **Wybierz** symbol sparowanego urządzenia.
    b. Z menu kontekstowego wybierz opcję **Prepare** (Przygotuj). Zostanie uruchomiony kreator ułatwiający przeprowadzenie procesu.

4. W kroku **Prepare Devices** (Przygotuj urządzenia):
    a. **Zaznacz** opcję **Supervise Devices** (Nadzoruj urządzenia).
    b. Kliknij przycisk **Next** (Dalej).

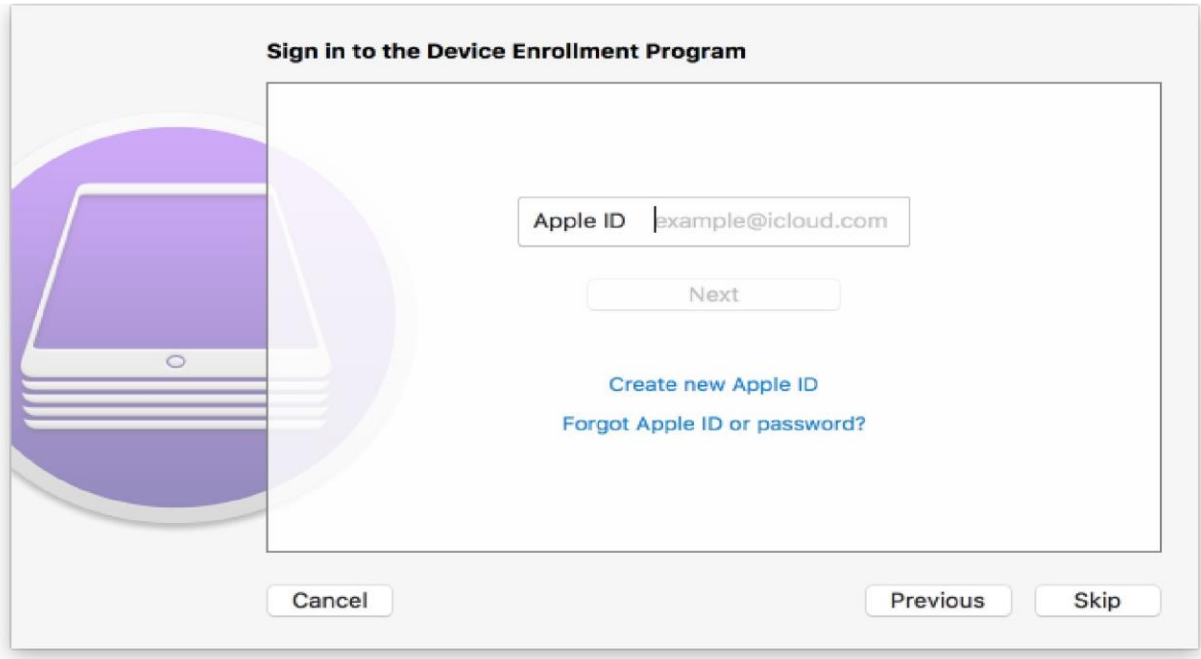


Rysunek 2-143 Opcje przygotowania urządzenia

5. W kroku **Enroll in MDM Server** (Zarejestruj na serwerze MDM):
    a. Upewnij się, że w menu rozwijanym **Server** (Serwer) wybrano opcję **Do not enroll in MDM** (Nie rejestruj w MDM).
    b. Kliknij przycisk **Next** (Dalej).

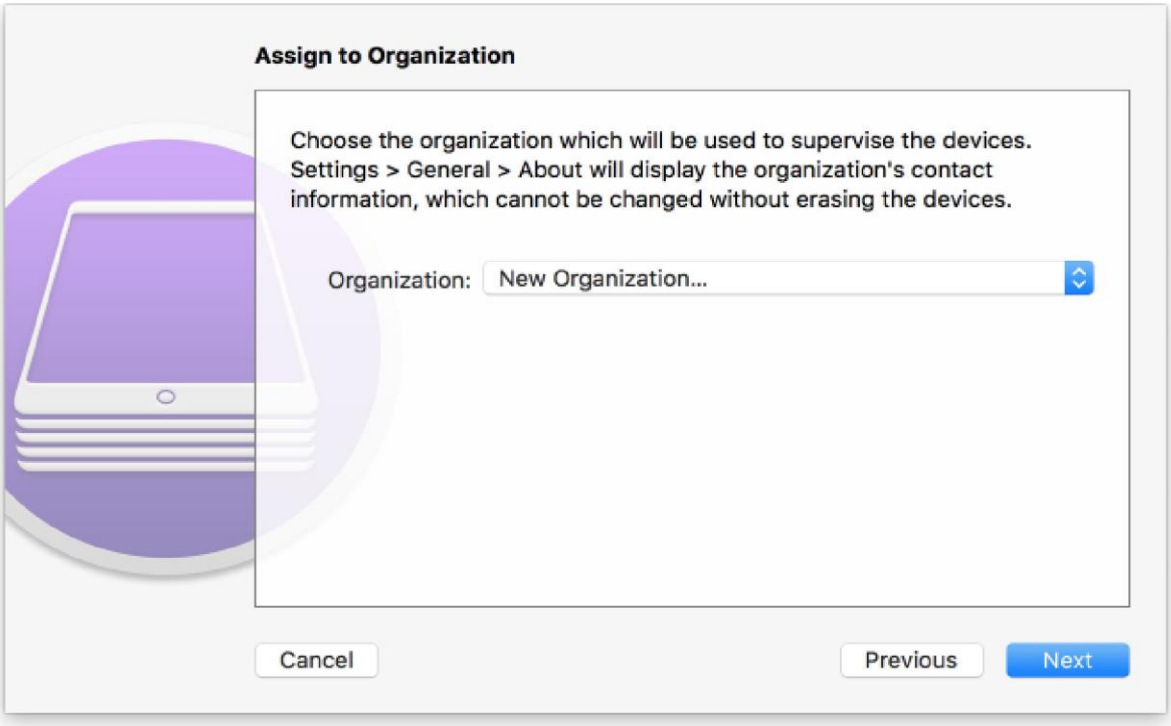
Rysunek 2-144 Wybór serwera MDM

6. W kroku **Sign into the Device Enrollment Program** (Zaloguj się do programu rejestracji urządzeń) naciśnij przycisk **Skip** (Pomiń).



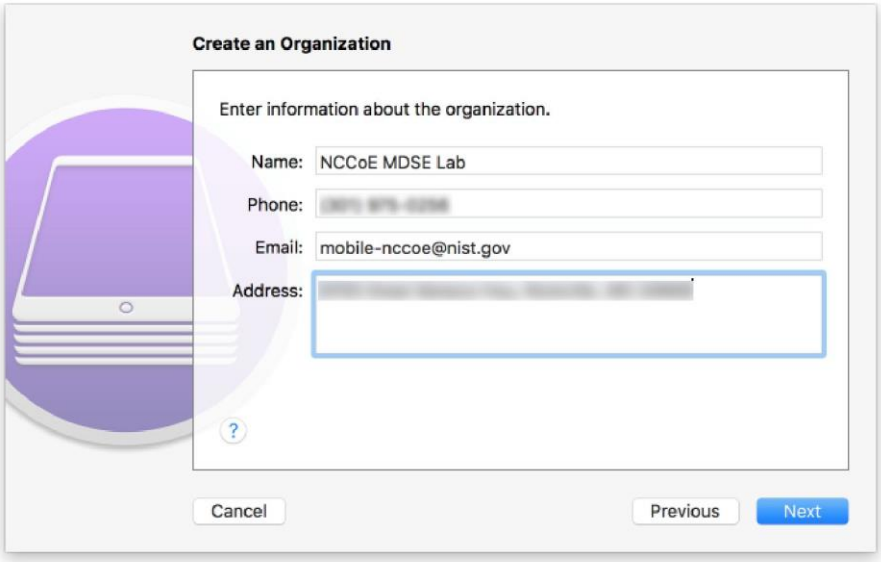
Rysunek 2-145 Logowanie do konta Apple

7. W kroku **Assign to Organization** (Przypisz do organizacji):
    a. Jeśli organizacja została utworzona wcześniej, kliknij przycisk **Next** (Dalej) i przejdź do kroku 9.
    b. Jeśli organizacja nie została jeszcze utworzona, z menu rozwijanego **Organization** (Organizacja) wybierz opcję **New Organization...** (Nowa organizacja...).



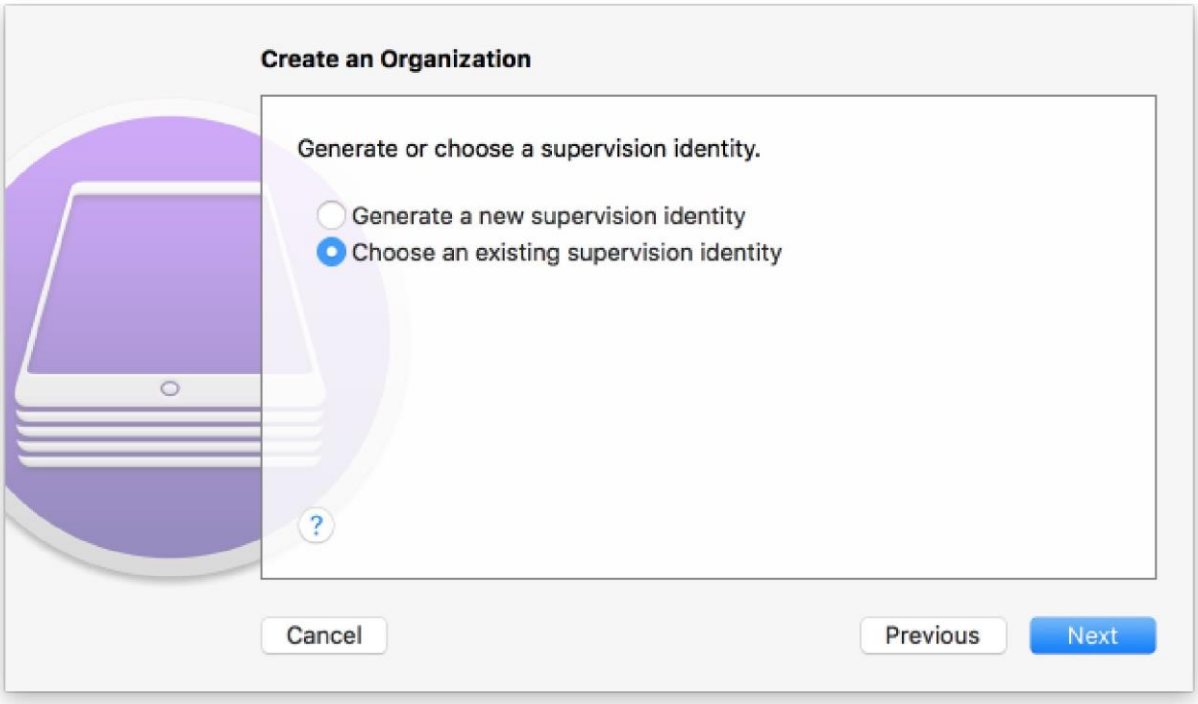
Rysunek 2-146 Okno dialogowe przypisywania organizacji

8. Na ekranie **Create an Organization** (Utwórz organizację):
    a. W polu **Name** (Nazwa) wprowadź nazwę organizacji.
    b. W polu **Phone** (Telefon) wprowadź numer pomocy technicznej odpowiedni dla danego programu mobilności.
    c. W polu **Email** wprowadź adres e-mail pomocy technicznej odpowiedni dla danego programu mobilności.
    d. W polu **Address** (Adres) wprowadź adres organizacji.
    e. Kliknij przycisk **Next** (Dalej).



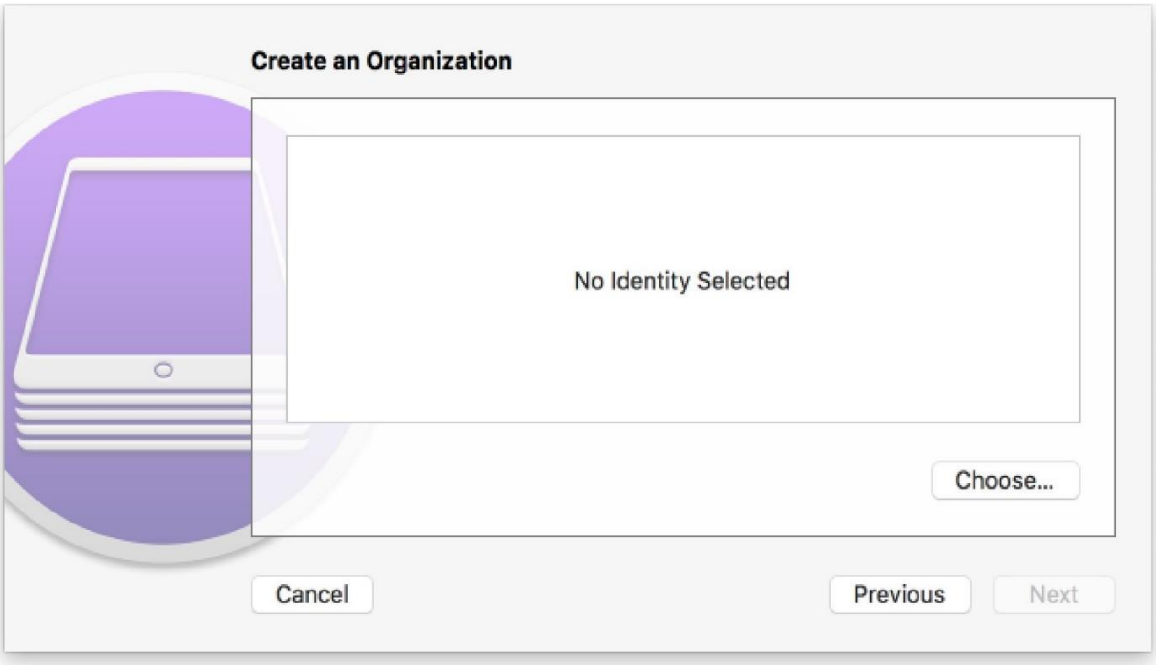
Rysunek 2-147 Tworzenie organizacji

9. Jeśli organizacja ustanowiła tożsamość cyfrową na potrzeby przełączania urządzeń w tryb nadzorowany:
    a. Przejdź do kroku 10. **Uwaga**: ta sama tożsamość cyfrowa musi być użyta dla każdego urządzenia.
    b. W przeciwnym razie przejdź do kroku 14.
10. Na ekranie **Create an Organization** (Utwórz organizację):
    a. Dla ustawienia **Generate or choose a supervision identity** (Wygeneruj lub wybierz tożsamość nadzorującą) wybierz opcję **Choose an existing supervision identity** (Wybierz istniejącą tożsamość nadzorującą).
    b. Kliknij przycisk **Next** (Dalej).



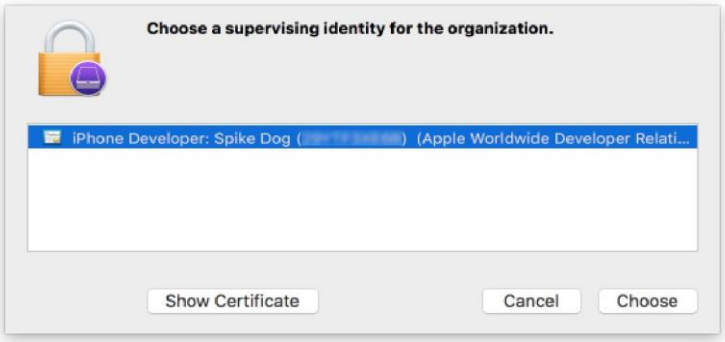
Rysunek 2-148 Konfiguracja tożsamości nadzorującej

11. Wybierz opcję **Choose...** (Wybierz...).



Rysunek 2-149 Wybór organizacji

12. W oknie dialogowym **Choose a supervising identity for the organization** (Wybierz tożsamość nadzorującą dla organizacji):
    a. **Wybierz** certyfikat cyfrowy z listy dostępnych w systemie.
    b. Kliknij przycisk **Choose** (Wybierz).

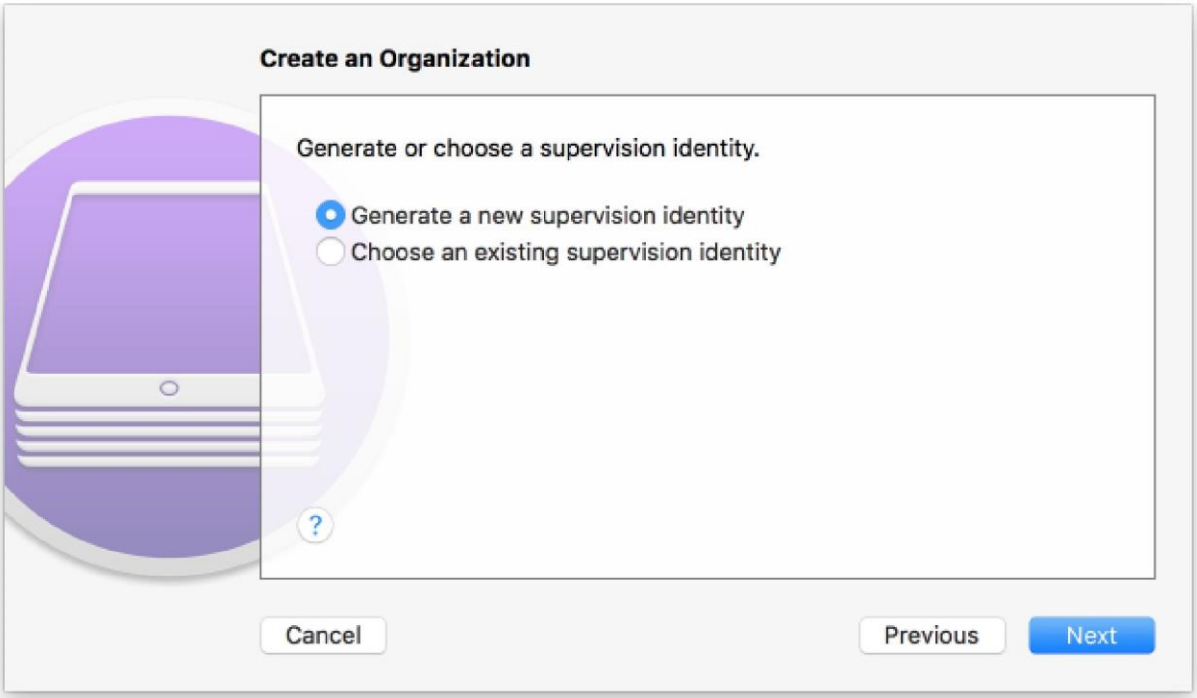


Rysunek 2-150 Wybór tożsamości nadzorującej

13. Na ekranie **Create an Organization** (Utwórz organizację) kliknij przycisk **Next** (Dalej).

Rysunek 2-151 Wybrana organizacja

14. Na ekranie **Create an Organization** (Utwórz organizację):
    a. Dla ustawienia **Generate or choose a supervision identity** (Wygeneruj lub wybierz tożsamość nadzorującą) wybierz opcję **Generate a new supervision identity** (Wygeneruj nową tożsamość nadzorującą).
    b. Kliknij przycisk **Next** (Dalej).



Rysunek 2-152 Konfiguracja tworzenia tożsamości nadzorującej dla Organizacji

15. W kroku **Configure iOS Setup Assistant** (Skonfiguruj asystenta konfiguracji iOS):

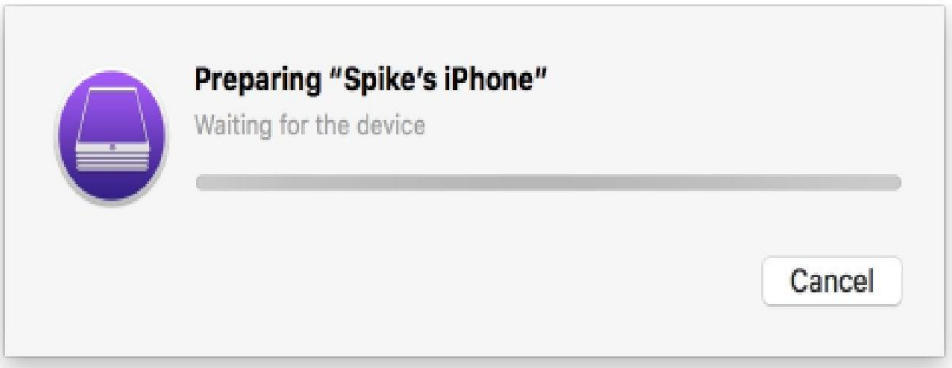
    a. Upewnij się, że z menu rozwijanego **Setup Assistant** (Asystent konfiguracji) wybrano opcję **Show only some steps** (Pokaż tylko niektóre kroki). Pojawią się dodatkowe opcje.

    b. Zaznacz pola wyboru **Privacy** (Prywatność), **Passcode** (Kod dostępu), **Apple ID** (Identyfikator Apple) i **Location Services** (Usługi lokalizacji).

    c. Kliknij przycisk **Prepare** (Przygotuj).

Rysunek 2-153 Ustawienia asystenta konfiguracji

16. Przygotowanie urządzenia i przełączenie go w tryb nadzorowany przez narzędzie **Configurator 2** zajmie kilka minut.

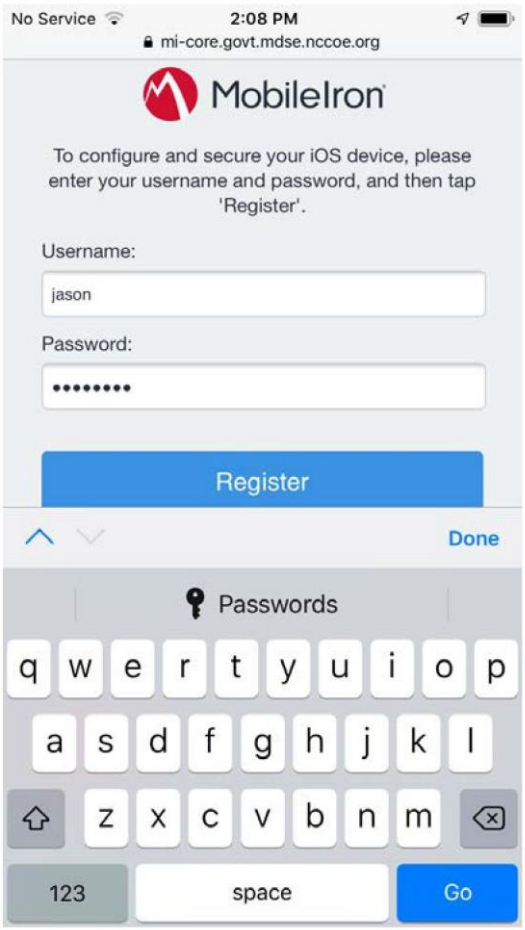


Rysunek 2-154 Oczekiwanie na iPhone'a

2.9.1.3. 2.9.1.3. REJESTRACJA W SYSTEMIE MOBILEIRON CORE

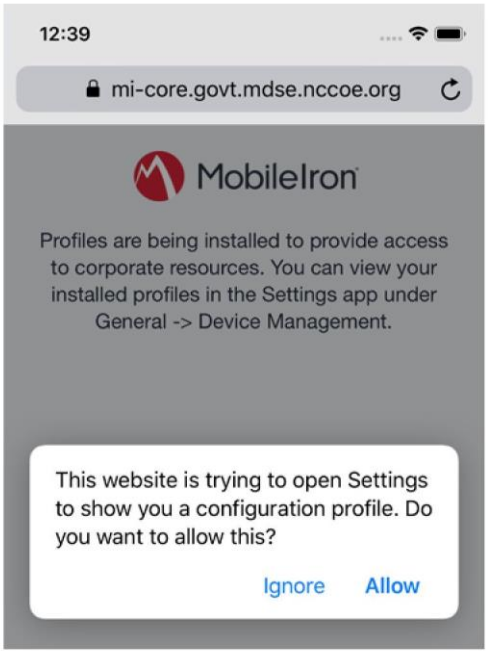
Poniższe kroki umożliwiają zarejestrowanie urządzenia z systemem iOS w trybie nadzorowanym w systemie MobileIron Core, który korzysta z procesu internetowego, a nie aplikacji Mobile@Work.

1. Korzystając z przeglądarki **Safari**, przejdź do strony **MobileIron Core**, wstawiając w adresie URL nazwę <FQDN> dla instancji systemu MobileIron Core danej organizacji. W naszym przykładowym wdrożeniu uzyskany w ten sposób adres URL to *https://mi-core.govt.mdse.nccoe.org/go*.



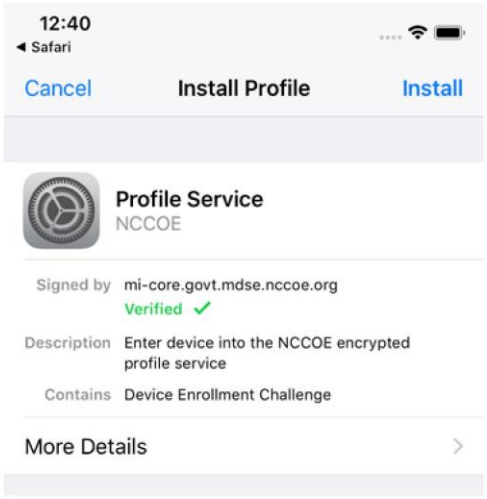
Rysunek 2-155 Strona rejestracji urządzenia z systemem iOS w systemie MobileIron

2. Po wyświetleniu **ostrzeżenia**, że witryna internetowa próbuje otworzyć aplikację **Settings** (Ustawienia) w celu wyświetlenia profilu konfiguracyjnego, kliknij przycisk **Allow** (Zezwól). Zostanie otwarta wbudowana aplikacja **Settings** (Ustawienia).



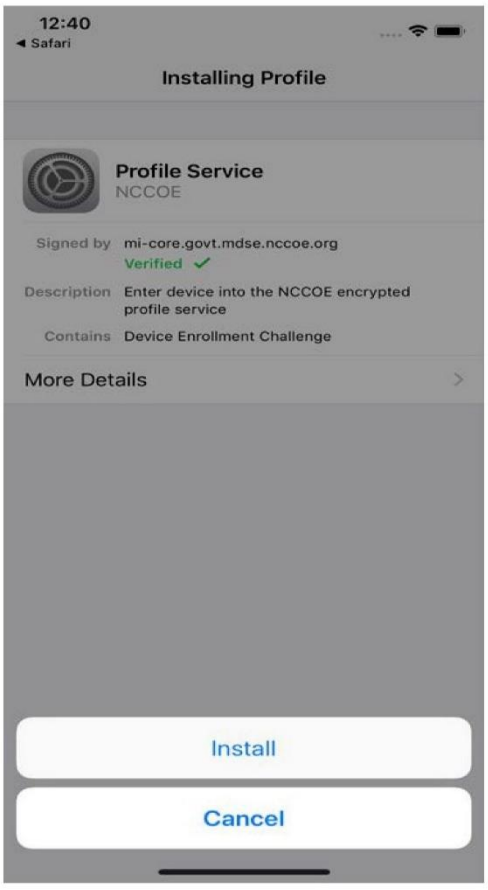
Rysunek 2-156 Potwierdzenie uruchomienia aplikacji Settings

3. Na ekranie **Settings** (Ustawienia) > **Install Profile** (Zainstaluj profil):
    a. Sprawdź, czy dla pola **Signed by** (Podpisane przez) wyświetlany jest wskaźnik **Verified** (Zweryfikowano), co oznacza, że tożsamość serwera została zweryfikowana.
    b. Wybierz opcję **Install** (Zainstaluj).



Rysunek 2-157 Instalacja profilu

4. Na ekranie **Installing Profile** (Instalowanie profilu) wybierz opcję **Install** (Zainstaluj).

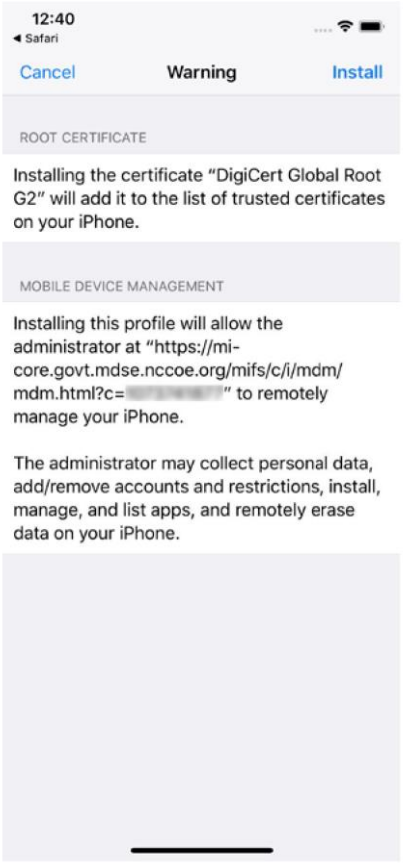


Rysunek 2-158 Instalacja profilu

5. Na ekranie **Warning** (Ostrzeżenie):

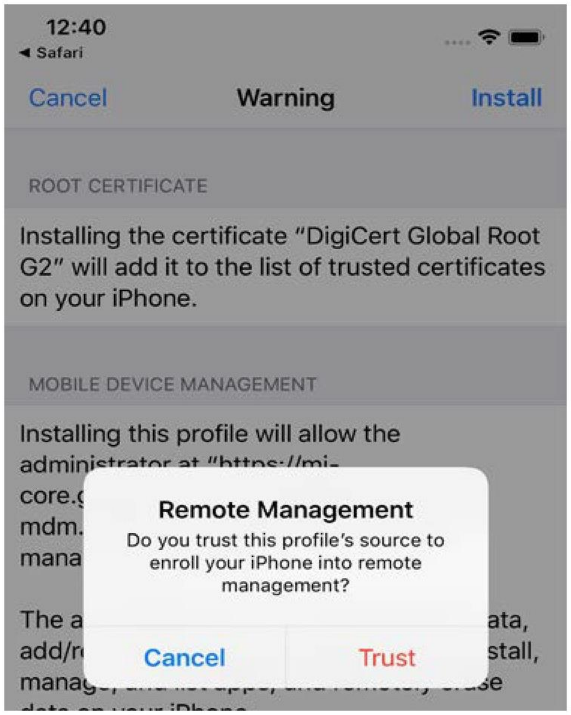
    a. Sprawdź, czy informacje w częściach **Root Certificate** (Certyfikat główny) i **MDM** są zgodne z informacjami dostarczonymi przez administratora urządzenia mobilnego.

    b. Wybierz opcję **Install** (Zainstaluj).



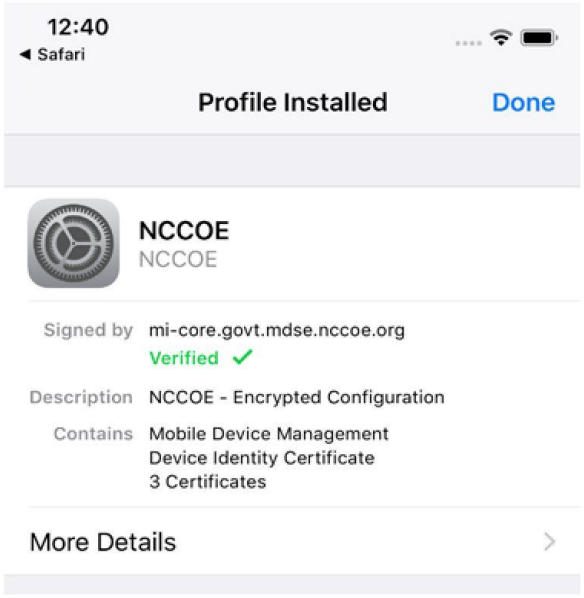
Rysunek 2-159 Ostrzeżenie dotyczące instalacji profilu

6. W oknie dialogowym **Remote Management** (Zdalne zarządzanie) wybierz opcję **Trust** (Zaufaj).



Rysunek 2-160 Potwierdzenie zaufania do instalowanego profilu

7. Na ekranie **Profile Installed** (Zainstalowany profil) wybierz opcję **Done** (Gotowe). Urządzenie jest teraz zarejestrowane w systemie MobileIron.



Rysunek 2-161 Potwierdzenie instalacji profilu

2.9.2. AKTYWACJA APLIKACJI LOOKOUT FOR WORK W SYSTEMIE IOS

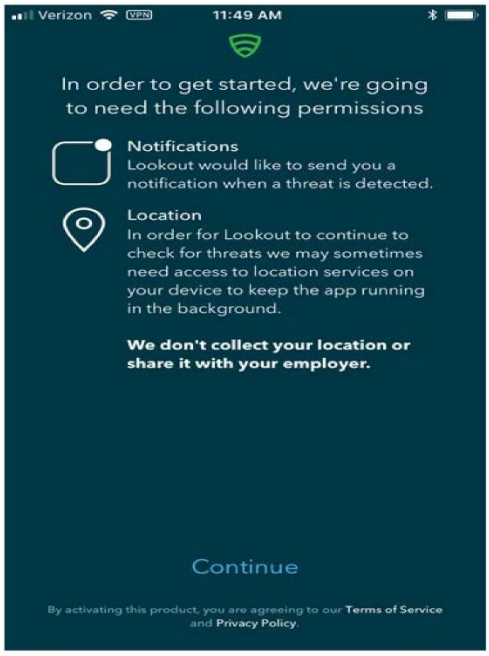
Konfiguracja aplikacji Lookout for Work (iOS) w katalogu aplikacji systemu MobileIron powoduje uwzględnienie pliku konfiguracyjnego podczas automatycznej instalacji.

Po uruchomieniu aplikacji wymagane jest wykonanie dodatkowych czynności w celu przyznania Lookout for Work uprawnień niezbędnych do zapewnienia optymalnej ochrony.

1. Uruchom aplikację **Lookout for Work**. Aktywacja odbywa się bez udziału użytkownika na **ekranie startowym**.

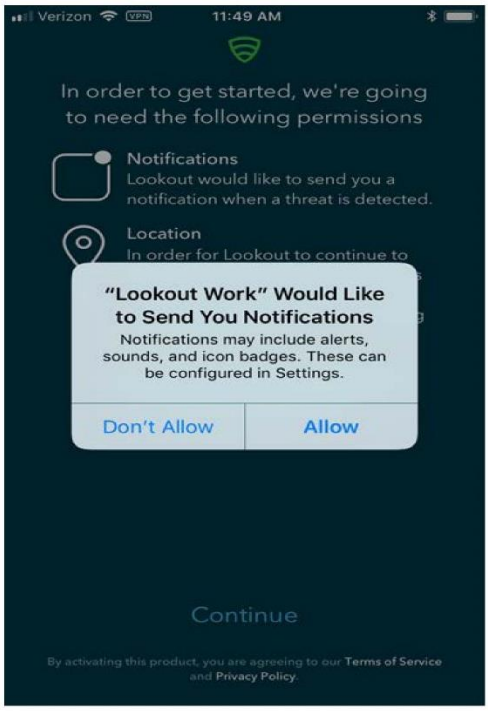
Rysunek 2-162 Ekran startowy aplikacji Lookout for Work

2. Na **ekranie powitalnym** wybierz opcję **Continue** (Kontynuuj).



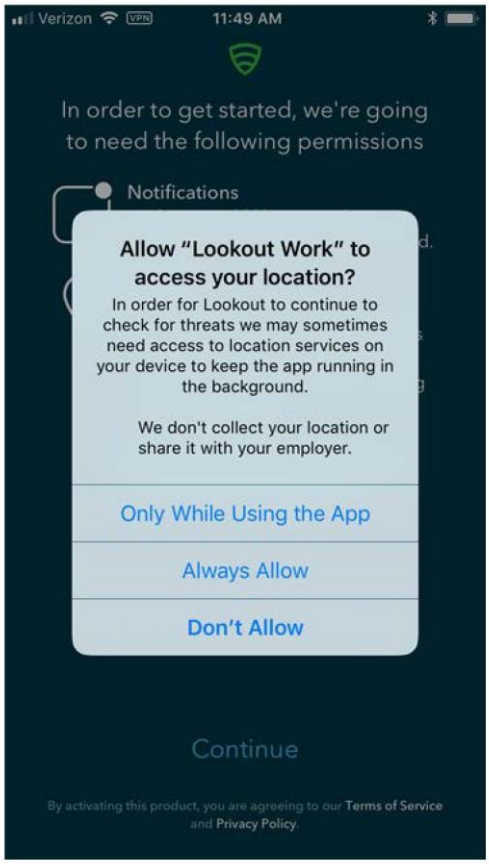
Rysunek 2-163 Informacja o uprawnieniach aplikacji Lookout for Work

3. W oknie dialogowym **"Lookout Work" Would Like to Send You Notifications** („Lookout Work” chce Ci wysyłać powiadomienia) wybierz opcję **Allow** (Zezwól).



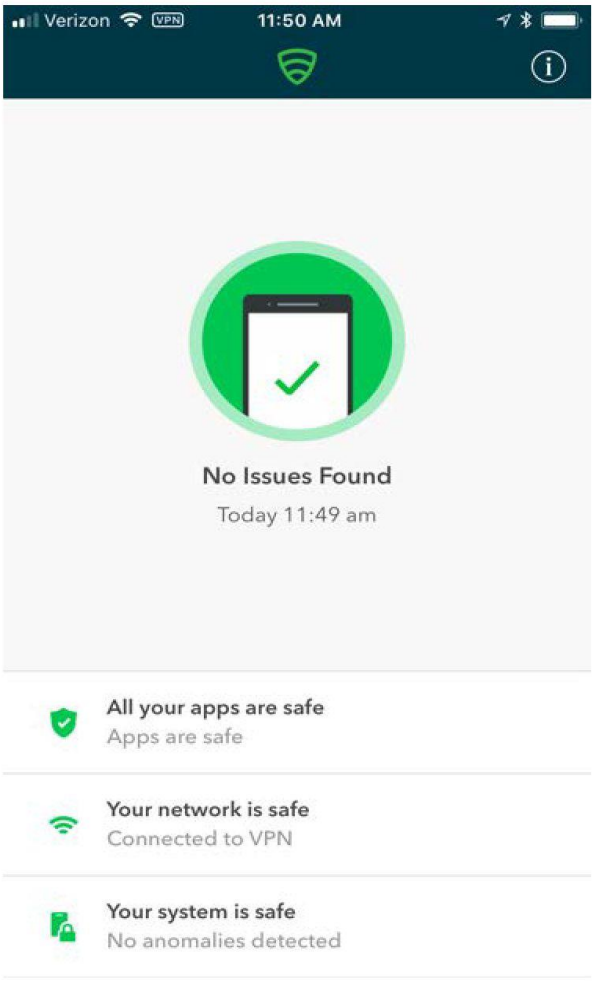
Rysunek 2-164 Monit o uprawnienia do wysyłania powiadomień

4. W oknie dialogowym **Allow "Lookout Work" to Access Your Location?** (Zezwolić „Lookout Work” na dostęp do Twojej lokalizacji?) wybierz opcję **Always Allow** (Zawsze zezwalaj).



Rysunek 2-165 Monit o dostęp do lokalizacji

5. Aplikacja **Lookout for Work** powinna automatycznie skanować aktywność urządzenia i aplikacji oraz przekazywać użytkownikowi informacje zwrotne.



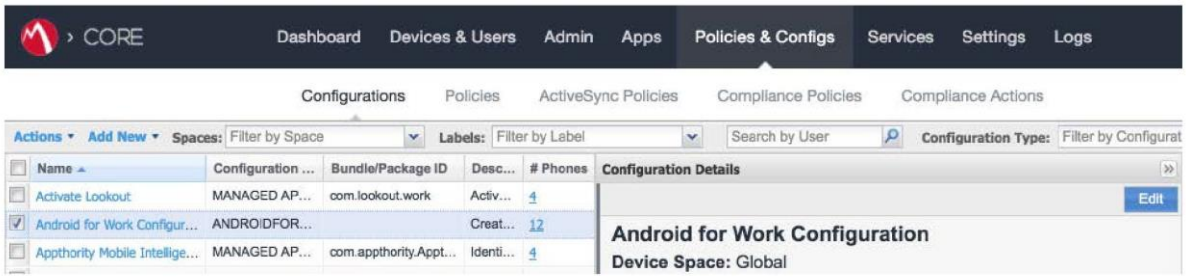
Rysunek 2-166 Ekran główny aplikacji Lookout for Work

2.9.3. WGRYWANIE PROFILU SŁUŻBOWEGO NA ZARZĄDZANE PRZEZ FIRMĘ URZĄDZENIA Z SYSTEMEM ANDROID

W tym scenariuszu urządzenia z systemem Android są wdrażane i zarządzane przez firmę za pośrednictwem profilu służbowego. Włączenie tej funkcji dla urządzeń obsługujących system AFW wymaga zmiany jego konfiguracji. Wymaga również, aby użytkownik urządzenia miał już osobiste konto Google w celu udostępnienia mu profilu służbowego. Nie jest ono tworzone w ramach procedury rejestracji urządzenia w systemie MobileIron Core.

2.9.3.1. AKTYWACJA PROFILU SŁUŻBOWEGO NA URZĄDZENIACH ZARZĄDZANYCH PRZEZ FIRMĘ

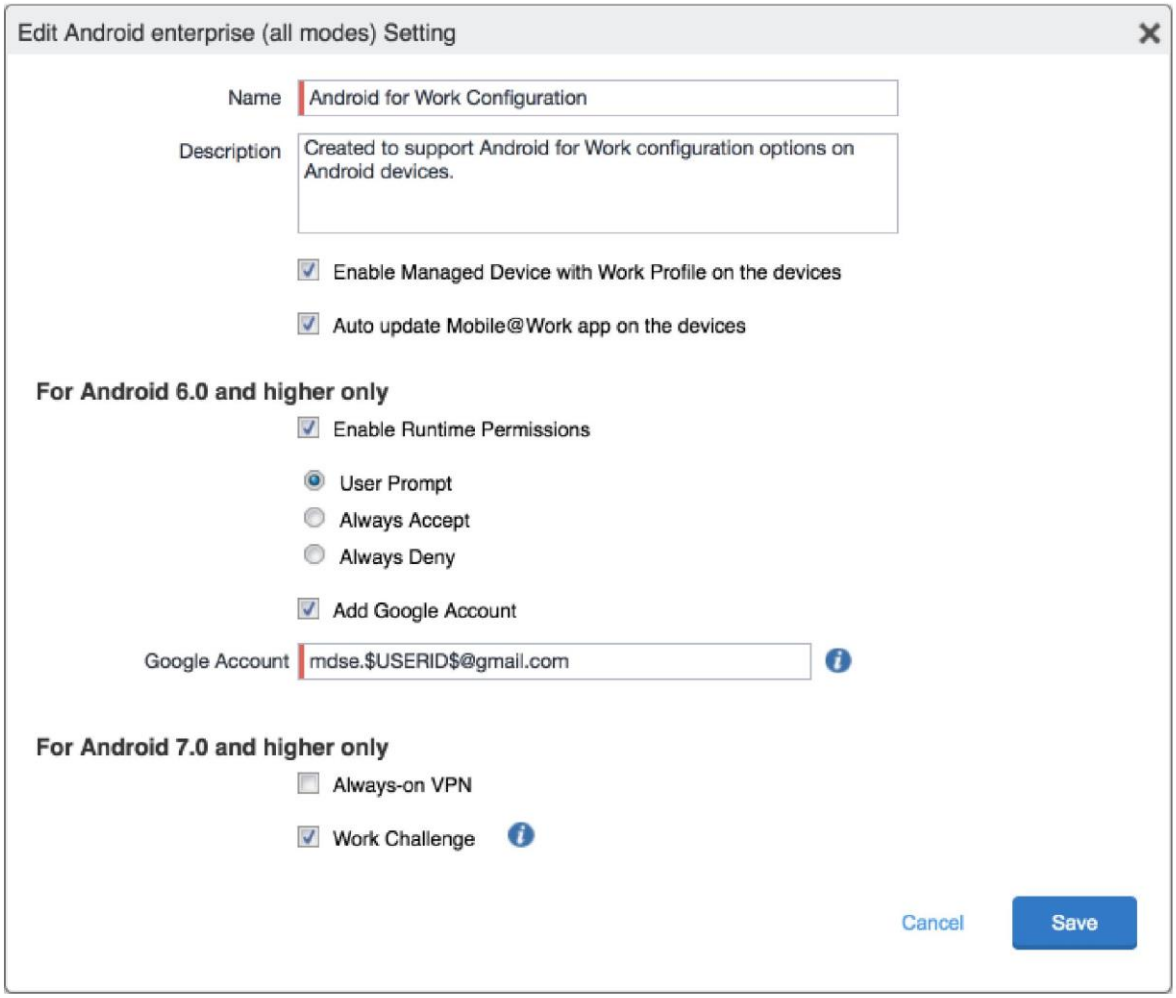
1. Na stronie **MobileIron Admin Portal** przejdź do części **Policies & Configs** (Zasady i konfiguracja) > **Configurations** (Konfiguracje).
2. **Zaznacz** pole wyboru w wierszu konfiguracji systemu **AFW**.
3. W panelu **Configuration Details** (Szczegóły konfiguracji) wybierz opcję **Edit** (Edytuj).



Rysunek 2-167 Konfiguracja protokołu AFW w systemie MobileIron

4. W oknie dialogowym **Edit Android enterprise (all modes) Setting** [Edytuj ustawienia systemu Android dla przedsiębiorstw (wszystkie tryby)]:
   a. Zaznacz opcję **Enable Managed Devices with Work Profile on the devices** (Włącz zarządzanie urządzeniem na urządzeniach z profilem służbowym).
   b. Zaznacz opcję **Add Google account** (Dodaj konto Google).
   c. W polu tekstowym **Google Account** (Konto Google) podaj prawidłowe konto w domenie Google. W naszym przykładowym wdrożeniu referencyjnym identyfikator użytkownika w systemie MobileIron, **gema**, został powiązany z adresem e-mail **mdse.gema@gmail.com**. Należy to zrobić dla każdego użytkownika. Lista zmiennych umożliwiających odpowiednie dostosowanie tego pola do istniejącej strategii zarządzania tożsamością znajduje się w dokumencie *MobileIron Core 9.4.0.0 Device Management Guide for AFW*.

d. Kliknij przycisk **Save** (Zapisz).

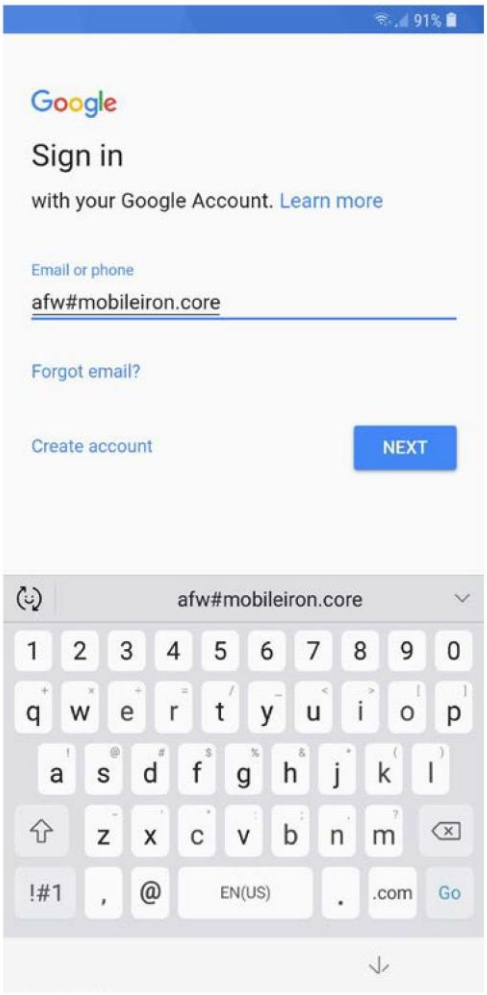


Rysunek 2-168 Konfiguracja systemu AFW

2.9.3.2. REJESTRACJA URZĄDZEŃ Z SYSTEMEM ANDROID

Poniższe kroki można wykonać tylko podczas pracy z urządzeniem z systemem Android, które nadal ma ustawienia fabryczne lub zostało do nich przywrócone.

1. Po wyświetleniu monitu o **zalogowanie się** przy użyciu konta Google:
   a. W polu **Email or phone** (E-mail lub telefon) wpisz **afw#mobileiron.core**.
   b. Kliknij przycisk **Next** (Dalej).

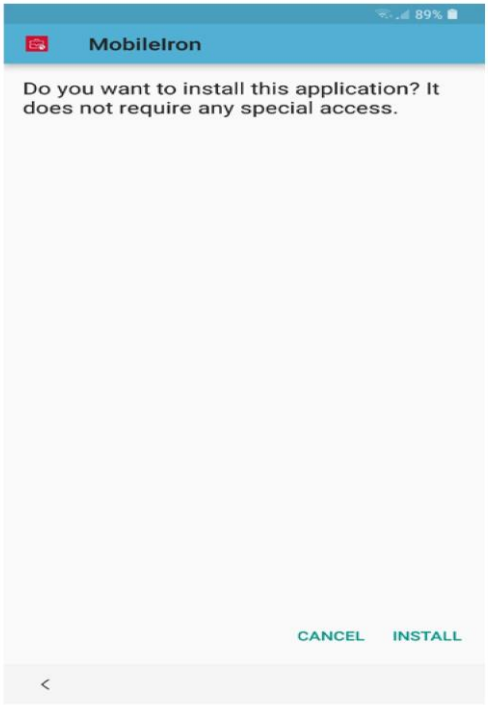


Rysunek 2-169 Proces rejestracji w systemie MobileIron

2. Gdy **AFW** wyświetli monit o zainstalowanie *Mobile@Work*, wybierz opcję **Install** (Zainstaluj). Spowoduje to pobranie klienta Mobile@Work na urządzenie.

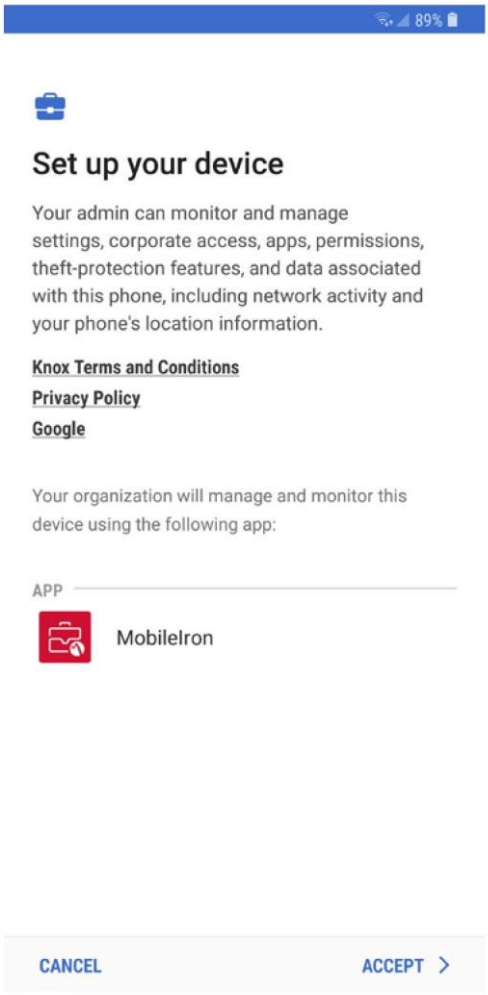
Rysunek 2-170 Rejestracja systemu AFW

3. Po wyświetleniu monitu o zainstalowanie aplikacji MobileIron wybierz opcję **Install** (Zainstaluj).



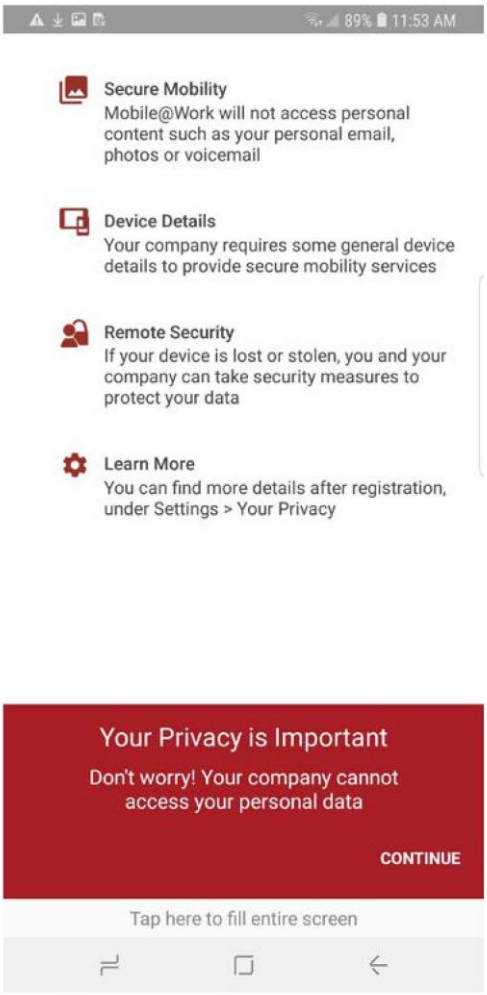
Rysunek 2-171 Instalacja aplikacji MobileIron

4. Na ekranie **Set up your device** (Skonfiguruj swoje urządzenie) wybierz opcję **Accept** (Zaakceptuj).



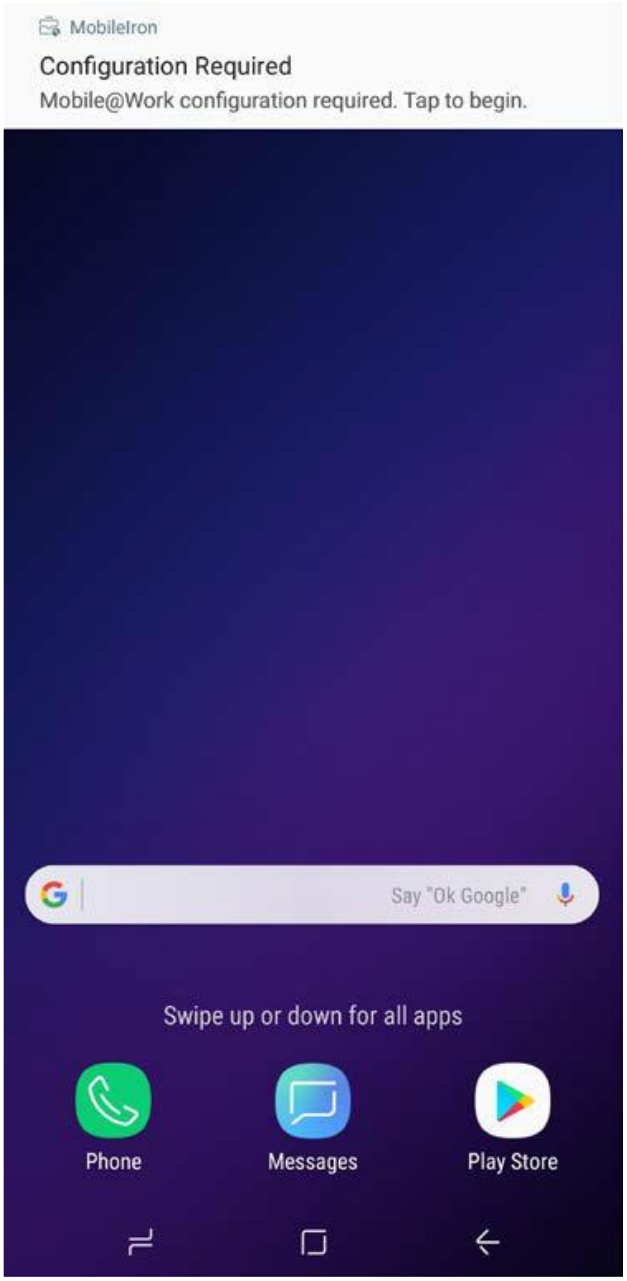
Rysunek 2-172 Akceptacja regulaminu AFW

5. Na tym ekranie znajdują się informacje o danych gromadzonych przez aplikację Mobile@Work i sposobie ich wykorzystania. Po zapoznaniu się z tymi informacjami wybierz opcję **Accept** (Zaakceptuj). Okno aplikacji Mobile@Work zostanie zminimalizowane i nastąpi powrót do ekranu głównego systemu operacyjnego.



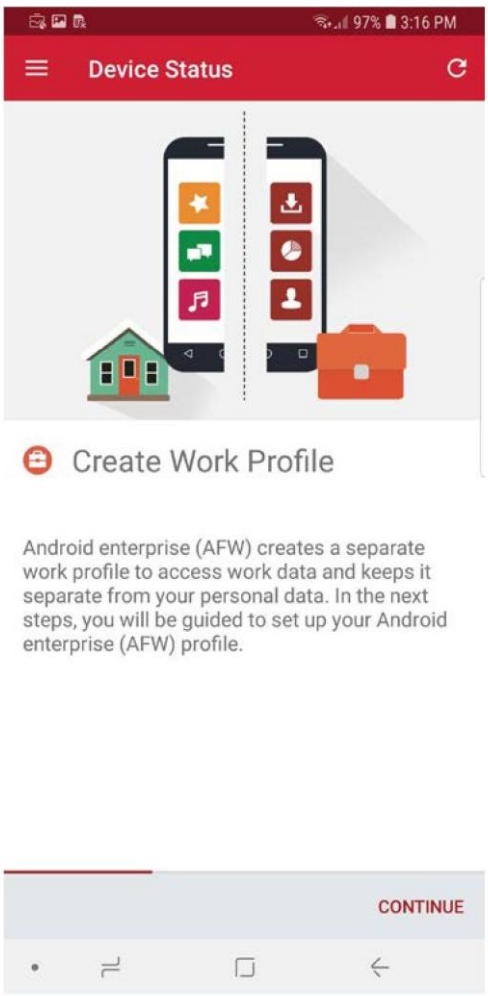
Rysunek 2-173 Informacje o ochronie prywatności w systemie MobileIron

6. Gdy system MobileIron wyśle powiadomienie **Configuration Required** (Wymagana konfiguracja), wybierz to **powiadomienie**.



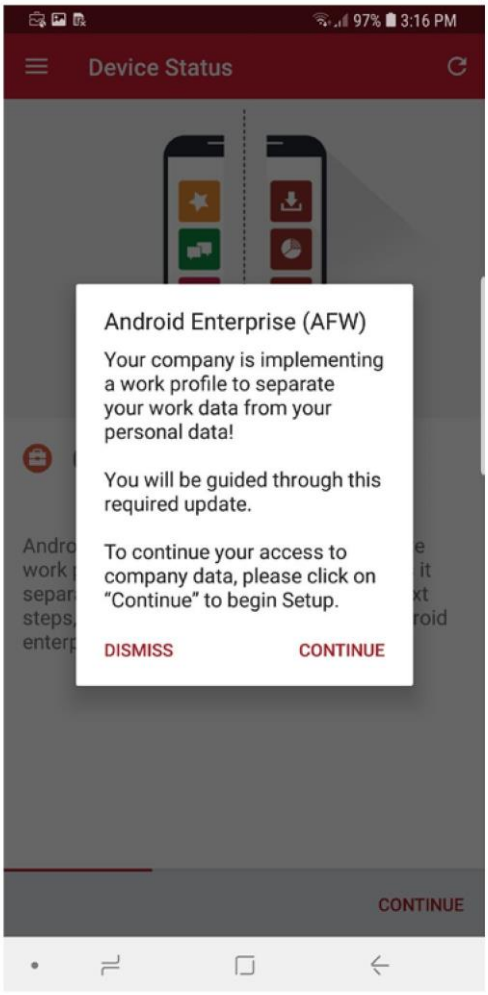
Rysunek 2-174 Powiadomienie o wymaganej konfiguracji systemu MobileIron

7. Na ekranie **Device Status** (Stan urządzenia) > **Create Work Profile** (Utwórz profil służbowy) wybierz opcję **Continue** (Kontynuuj).



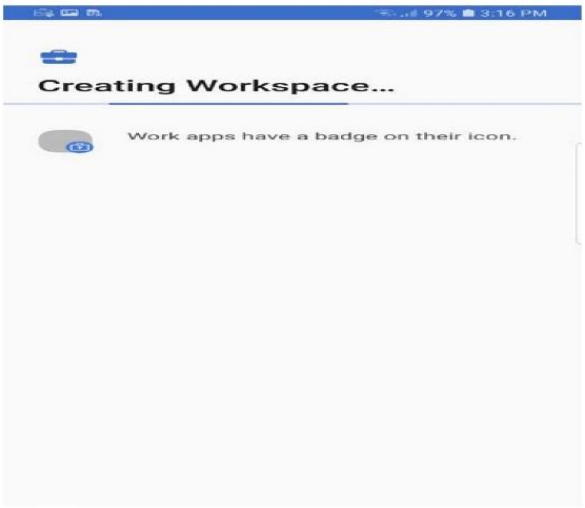
Rysunek 2-175 Stan urządzenia w systemie MobileIron

8. Po wyświetleniu monitu **AFW** wybierz opcję **Continue** (Kontynuuj).



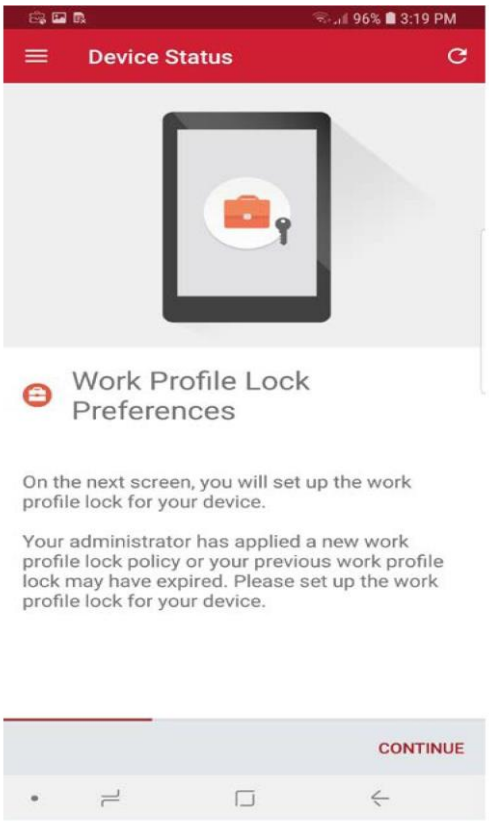
Rysunek 2-176 Konfiguracja systemu AFW

9. **AFW** powiadamia użytkownika o utworzeniu osobistej przestrzeni roboczej. Na kolejnych dwóch ekranach zostaną powtórzone kroki 3 i 4 opisane powyżej.



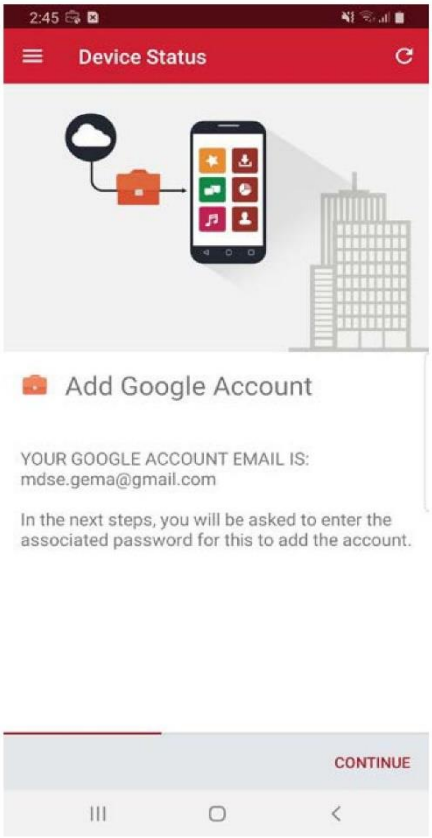
Rysunek 2-177 Tworzenie przestrzeni roboczej w systemie AFW

10. Na ekranie **Device Status** (Stan urządzenia) > **Work Profile Lock Preferences** (Preferencje blokady profilu służbowego) wybierz opcję **Continue** (Kontynuuj).



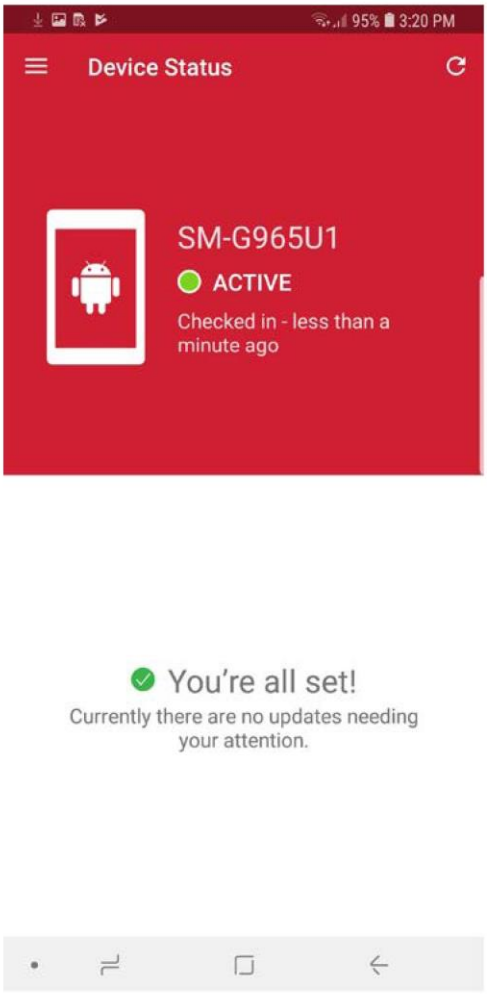
Rysunek 2-178 Preferencje blokady profilu służbowego w systemie MobileIron

11. Użytkownik zostanie poproszony o utworzenie kodu dostępu w celu ochrony kontenera AFW.
12. Na ekranie **Device Status** (Stan urządzenia) > **Add Google Account** (Dodaj konto Google) wybierz opcję **Continue** (Kontynuuj).



Rysunek 2-179 Konfiguracja konta Google w systemie MobileIron

13. Użytkownik zostanie poproszony o uwierzytelnienie przy użyciu tego samego konta w domenie Google, które zostało przypisane do jego konta w systemie MobileIron na podstawie adresu e-mail ustawionego w konfiguracji AFW w MobileIron Core. W naszym przykładowym wdrożeniu powiązane konto Google to **mdse.gema@gmail.com**.
14. Gdy aplikacja Mobile@Work uzyska dostęp do konta użytkownika, powinien się pojawić ekran **Device Status** (Stan urządzenia). Urządzenie zostało pomyślnie zarejestrowane w systemie MobileIron.



Rysunek 2-180 Stan urządzenia w systemie MobileIron

ZAŁĄCZNIK A LISTA AKRONIMÓW

Wybrane akronimy i skróty użyte w treści niniejszego opracowania zostały rozwinięte i zdefiniowane poniżej.

Dodatkowo patrz: **NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa***

Akronim	Terminologia angielska	Terminologia polska
AD	Active Directory	Usługa Active Directory
AFW	Android for Work	Android for Work
API	Application Programming Interface	Interfejs programistyczny aplikacji
CA	Certificate Authority	Urząd certyfikacji
COPE	Corporate-Owned Personally-Enabled	Organizacyjne urządzenia mobilne obsługiwane osobiście przez użytkowników
DMZ	Demilitarized Zone	Strefa zdemilitaryzowana
DN	Distinguished Name	Nazwa wyróżniająca
DNS	Domain Name System	System nazw domen
DPC	Derived Personal Identity Verification Credential	Poświadczenie certyfikatu identyfikacji tożsamości
EMM	Enterprise Mobility Management	Zarządzanie mobilnością w przedsiębiorstwie
FQDN	Fully Qualified Domain Name	W pełni kwalifikowana nazwa domeny
GOVT	Government	Rząd
HTTP	Hypertext Transfer Protocol	Protokół http
HTTPS	Hypertext Transfer Protocol Secure	Protokół https
ID	Identifier	Identyfikator
IMEI	International Mobile Equipment Identity	Międzynarodowy identyfikator urządzenia mobilnego
IP	Internet Protocol	Protokół internetowy
LAN	Local Area Network	Lokalna sieć komputerowa
LDAP	Lightweight Directory Access Protocol	Protokół LDAP
MDM	Mobile Device Management	Zarządzanie urządzeniami mobilnymi

MDS	Mobile Device Security	Bezpieczeństwo urządzeń mobilnych:
MES	Mobile Endpoint Security	Bezpieczeństwo mobilnych punktów końcowych
MTP	Mobile Threat Posture	Poziom zagrożeń mobilnych
NAT	Network Address Translation	Translacja adresów sieciowych
NCCoE	National Cybersecurity Center of Excellence	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology	Narodowy Instytut Standaryzacji i Technologii
NTP	Network Time Protocol	Protokół synchronizacji czasu
OVA	Open Virtualization Appliance	Otwarte urządzenie wirtualizacyjne
PLIST	Property List	Lista właściwości
SCEP	Simple Certificate Enrollment Protocol	Prosty protokół rejestracji certyfikatów
SSH	Secure Shell	Protokół SSH
SSID	Service Set Identifier	Identyfikator zestawu usług
SSL	Secure Sockets Layer	Protokół SSL
TLS	Transport Layer Security	Bezpieczeństwo warstwy transportowej
URL	Uniform Resource Locator	Standard URL
USB	Universal Serial Bus	Uniwersalna magistrala szeregowa
VLAN	Virtual Local Area Network	Wirtualna sieć lokalna
VPN	Virtual Private Network	Wirtualna sieć prywatna
WAN	Wide Area Network	Rozległa sieć informatyczna

ZAŁĄCZNIK B SŁOWNIK

Poniżej zostały przedstawione definicje wybranych terminów użytych w treści niniejszej publikacji. Niektóre definicje zostały opatrzone odnośnikami do źródeł.

Dodatkowo patrz: **NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa***

Terminologia angielska	Terminologia polska	Definicja
Application Programming Interface (API)	Interfejs programistyczny aplikacji	Punkt dostępu do systemu lub funkcja biblioteczna, która ma dobrze zdefiniowaną składnię i jest dostępna z programów aplikacyjnych lub kodu użytkownika w celu zapewnienia dobrze zdefiniowanej funkcjonalności [1].
App-Vetting Process	Proces weryfikacji aplikacji	Proces weryfikacji, czy aplikacja spełnia wymagania bezpieczeństwa organizacji. Proces weryfikacji aplikacji obejmuje jej testowanie oraz działania związane z jej zatwierdzeniem lub odrzuceniem [2].
Authenticate	Uwierzytelnianie	Weryfikacja tożsamości użytkownika, procesu lub urządzenia. Często traktowana jako warunek wstępny udzielenia dostępu do zasobów w systemie informacyjnym [3].
Certificate	Certyfikat	Struktura danych, która zawiera identyfikatory podmiotu, jego klucz publiczny (w tym wskazanie powiązanego zestawu parametrów domeny) i ewentualnie inne informacje, wraz z podpisem na tym zestawie danych, który jest generowany przez zaufaną stronę, tj. ośrodek certyfikacji, wiążąc w ten sposób klucz publiczny z zawartymi identyfikatorami [4].
Certificate Authority (CA)	Urząd certyfikacji	Zaufany podmiot, który wydaje i unieważnia certyfikaty klucza publicznego [5].

Terminologia angielska	Terminologia polska	Definicja
Corporate-Owned Personally-Enabled (COPE)	Urządzenia będące własnością firmy/organizacji wykorzystywane przez pracowników również do celów prywatnych. Organizacyjne urządzenia mobilne obsługiwane osobiście przez użytkowników	Urządzenie będące własnością przedsiębiorstwa i przydzielone pracownikowi. Zarówno przedsiębiorstwo, jak i pracownik mogą instalować aplikacje na urządzeniu.
Demilitarized Zone (DMZ)	Demilitarized Zone (DMZ) (Strefa zdemilitaryzowana)	Interfejs na zaporze routera, który jest podobny do interfejsów znajdujących się po chronionej stronie zapory. Ruch przechodzący między DMZ a innymi interfejsami po chronionej stronie zapory nadal przechodzi przez zaporę i mogą dla niego obowiązywać zasady ochrony zapory [6].
Derived Personal Identity Verification (PIV)	Poświadczenie certyfikatu identyfikacji tożsamości	Poświadczenie wydane na podstawie dowodu posiadania i kontroli karty PIV, aby nie powielać procesu potwierdzania tożsamości zdefiniowanego w dokumencie [SP 800-63-2]. Pochodny token poświadczenia PIV to token sprzętowy lub programowy, który zawiera pochodne poświadczenie PIV [7].
Hypertext Transfer Protocol (HTTP)	Protokół http	Standardowa metoda komunikacji między klientami a serwerami sieci Web [8].
Hypertext Transfer Protocol Secure (HTTPS)	Protokół https	Komunikacja HTTP przesyłana za pomocą protokołu TLS [9].
Internet Protocol (IP) addresses	Adres IP	Standardowy protokół transmisji danych od źródła do miejsca docelowego w pakietowych sieciach komunikacyjnych i wzajemnie połączonych systemach takich sieci [10].

Terminologia angielska	Terminologia polska	Definicja
Lightweight Directory Access Protocol (LDAP)	Protokół LDAP	Protokół dostępu do katalogów. W tym dokumencie termin LDAP odnosi się do protokołu zdefiniowanego w dokumencie RFC 1777, który jest również znany jako LDAP V2. LDAP V2 opisuje nieuwierzytelnione mechanizmy pobierania danych [11].
Local Area Network (LAN)	Lokalna sieć komputerowa	Grupa komputerów i innych urządzeń rozproszonych na stosunkowo ograniczonym obszarze i powiązanych łączem komunikacyjnym, które umożliwia każdemu urządzeniu interakcję z dowolnym innym urządzeniem w sieci [12].
Mutual Authentication	Uwierzytelnianie wzajemne	Proces wzajemnej weryfikacji obu podmiotów zaangażowanych w transakcję [13].
Passphrase	Fraza zabezpieczająca	Fraza zabezpieczająca to zapamiętany sekret składający się z sekwencji słów lub innego tekstu, którego użytkownik używa do uwierzytelnienia swojej tożsamości. Fraza zabezpieczająca jest podobna w użyciu do hasła, ale zazwyczaj jest dłuższa w celu zwiększenia poziomu bezpieczeństwa [14].
Personal Identity Verification (PIV)	Certyfikat identyfikacji tożsamości	Fizyczny przedmiot (np. dowód tożsamości, „inteligentna” karta) wydany osobie, na którym przechowywane są dane uwierzytelniające tożsamość (np. zdjęcie, klucze kryptograficzne, zdigitalizowane odciski palców), dzięki czemu deklarowana tożsamość posiadacza karty może zostać zweryfikowana w oparciu o dane uwierzytelniające przechowywane przez inną osobę (czytelne i weryfikowalne przez człowieka) lub zautomatyzowany proces (czytelne i weryfikowalne przez komputer). Wymagania dotyczące PIV zostały określone w normie FIPS PUB 201 [15].

Terminologia angielska	Terminologia polska	Definicja
Risk Analysis	Analiza ryzyka	Proces identyfikacji zagrożeń dla bezpieczeństwa systemu i określania prawdopodobieństwa ich wystąpienia, wynikających z nich skutków oraz dodatkowych zabezpieczeń, które mogą je złagodzić. Jest to część zarządzania ryzykiem i synonim szacowania ryzyka [16].
Risk Assessment	Szacowanie ryzyka	Proces identyfikacji zagrożeń dla działalności organizacji (w tym misji, funkcji, wizerunku, reputacji), aktywów organizacji, osób fizycznych, innych organizacji i państwa, wynikających z działania systemu informacyjnego [17].
Root Certificate Authority (CA)	Główny ośrodek certyfikacji	W hierarchicznej infrastrukturze klucza publicznego (PKI) ośrodek certyfikacji (CA), którego klucz publiczny służy jako najbardziej zaufane dane (tj. początek ścieżek zaufania) dla domeny bezpieczeństwa [18].

ZAŁĄCZNIK C REFERENCJE

	NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[11]
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

[11] Narodowe Standardy Cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl (www.gov.pl)

Tłumaczenie

NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61

	PUBLIKACJE ANGLOJĘZYCZNE[12]
[1]	National Institute of Standards and Technology (NIST). Information Technology Laboratory (ITL) Glossary, "Application Programming Interface Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Application_Programming_Interface.
[2]	NIST. ITL Glossary, "App-Vetting Process," [Online]. Available: https://csrc.nist.gov/glossary/term/App Vetting Process.
[3]	NIST. ITL Glossary, "Authenticate Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/authenticate.
[4]	NIST. ITL Glossary, "Certificate Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/certificate.
[5]	NIST. ITL Glossary, "Certificate Authority (CA) Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Certificate_Authority.
[6]	NIST. ITL Glossary, "Demilitarized Zone (DMZ) Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/demilitarized_zone.
[7]	NIST. ITL Glossary, "Derived Personal Identity Verification (PIV) Credential Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Derived_PIV_Credential.
[8]	NIST. ITL Glossary, "Hypertext Transfer Protocol (HTTP) Definition," [Online]. Available: https:// csrc.nist.gov/glossary/term/HTTP.
[9]	NIST. ITL Glossary, "Hypertext Transfer Protocol over Transport Layer Security Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Hypertext_Transfer_Protocol_over_Transport_Layer_Security.
[10]	NIST. ITL Glossary, "Internet Protocol (IP) Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/internet_protocol.

[12] Publikacje angielski zostały podane w celach uzupełniających dla osób zainteresowanych.

Tłumaczenie

[11] NIST. ITL Glossary, "Lightweight Directory Access Protocol Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Lightweight_Directory_Access_Protocol.

[12] NIST. ITL Glossary, "Local Area Network (LAN) Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Local_Area_Network.

[13] NIST. ITL Glossary, "Mutual Authentication Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/mutual_authentication.

[14] NIST. ITL Glossary, "Passphrase Definition," [Online]. Available: https://csrc.nist.gov/glossary/term/Passphrase.

[15] NIST. ITL Glossary, "Personal Identity Verification (PIV)," [Online]. Available: https://csrc.nist.gov/glossary/term/personal_identity_verification.

[16] NIST. ITL Glossary, "Risk Analysis," [Online]. Available: https://csrc.nist.gov/glossary/term/risk analysis.

[17] NIST. "NIST Special Publication 800-39, Managing Information Security Risk," March 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

[18] NIST. "NIST Special Publication 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure," February 2001. [Online]. Available:

https://nvlpubs.nist.gov/nipubs/Legacy/SP/nistspecialpublication800-32.pdf.