

Dokumentacija Proget

1. Strona główna
2. Konsola Proget
3. Przewodnik Administratora
4. Logowanie
5. Pulpit
6. Moja Karta
7. Urządzenia
8. Atrybuty
9. Certyfikaty
10. Logi Audytowe
11. Kopie Zapasowe
12. Ustawienia
13. Graf zależności
14. Użytkownicy
15. Dodawanie użytkownika z Microsoft Entra ID
16. Dodawanie użytkownika z LDAP
17. Dodawanie użytkownika lokalnego
18. Kopie zapasowe użytkownika
19. Aktywacje
20. Ręczna
21. Automatyczna
22. Szablony
23. Konfiguracja szablonu
24. Własna EULA
25. Konfiguracja EULA
26. Urządzenia
27. Aktywacje
28. Android Enterprise Device Owner
29. Hasło serwisowe
30. Android Enterprise Profile Owner (COPE)
31. Hasło serwisowe
32. Android
33. Hasło serwisowe
34. iOS (Tryb nadzorowany)
35. macOS
36. Windows

- 37. [Zakładki urządzeń](#)
- 38. [Podstawowe](#)
- 39. [Polityka](#)
- 40. [Profile](#)
- 41. [Aplikacje](#)
- 42. [Lokalizacja](#)
- 43. [Kopie zapasowe](#)
- 44. [Logi audytowe](#)
- 45. [Zadania](#)
- 46. [Graf zależności](#)
- 47. [File Manager](#)
- 48. [Raporty](#)
- 49. [Eksport](#)
- 50. [Konta użytkownika](#)
- 51. [Raporty o błędach systemowych](#)
- 52. [Zdjęcia z blokady](#)
- 53. [Użytkownicy](#)
- 54. [Grupy](#)
- 55. [Priorytety grup](#)
- 56. [Wybrana grupa](#)
- 57. [Zarządzaj filtrem](#)
- 58. [Język zapytań Proget \(PQL\)](#)
- 59. [Aplikacje](#)
- 60. [Dodaj aplikacje](#)
- 61. [Pojedyncza aplikacja Android](#)
- 62. [Pojedyncza aplikacja Android z pliku](#)
- 63. [Pojedyncza aplikacja iOS](#)
- 64. [Polityki](#)
- 65. [Android Enterprise Device Owner](#)
- 66. [Android Enterprise Profile Owner](#)
- 67. [Android](#)
- 68. [iOS](#)
- 69. [macOS](#)
- 70. [Windows](#)
- 71. [Profile](#)
- 72. [ActiveSync](#)

73. [APN](#)
74. [Konfiguracja Android Enterprise](#)
75. [Konfiguracja Samsung](#)
76. [Konfiguracja iOS](#)
77. [Apple Business Manager](#)
78. [Apple Update](#)
79. [Reguły aplikacji](#)
80. [Android Enterprise - przestrzeń służbowa](#)
81. [Android Enterprise - przestrzeń prywatna](#)
82. [iOS \(Tryb nadzorowany\)](#)
83. [Kopia zapasowa](#)
84. [Kontakty służbowe](#)
85. [Dokumenty firmowe](#)
86. [Certyfikat](#)
87. [Plik](#)
88. [Szablon](#)
89. [SCEP](#)
90. [Mapowanie certyfikatu](#)
91. [Łączność](#)
92. [Custom Apple Configuration](#)
93. [Geofencing](#)
94. [IMAP/POP](#)
95. [Kiosk](#)
96. [Android](#)
97. [Pojedyncza aplikacja](#)
98. [Wiele aplikacji](#)
99. [iOS](#)
100. [Lokalizacja](#)
101. [MTP](#)
102. [SCEP](#)
103. [Urządzenie współdzielone](#)
104. [VPN](#)
105. [Proget IPsec](#)
106. [IPsec](#)
107. [IKEv2](#)
108. [L2TP](#)

- 109. [Custom SSL](#)
- 110. [Tapeta](#)
- 111. [Wi-Fi](#)
- 112. [Etykiety](#)
- 113. [Logi audytowe](#)
- 114. [Zadania](#)
- 115. [Serwis](#)
- 116. [Aktualizacja](#)
- 117. [Historia serwisu](#)
- 118. [Hasło serwisowe](#)
- 119. [Bezpieczeństwo](#)
- 120. [Raporty](#)
- 121. [Lista raportów](#)
- 122. [Generuj raporty](#)
- 123. [Konfiguracja](#)
- 124. [Dodaj konfiguracje](#)
- 125. [Ustawienia](#)
- 126. [Kontrola dostępu](#)
- 127. [Dozwolone karty SIM](#)
- 128. [Lista](#)
- 129. [Zarządzaj dozwolonymi kartami SIM](#)
- 130. [Operacje](#)
- 131. [Audyt i logowanie](#)
- 132. [Menedżer certyfikatów](#)
- 133. [CAs](#)
- 134. [Certyfikaty użytkownika](#)
- 135. [Zewnętrzne certyfikaty](#)
- 136. [Connector](#)
- 137. [Gateway](#)
- 138. [Ogólne](#)
- 139. [LDAP](#)
- 140. [Microsoft Entra ID](#)
- 141. [Konfiguracje użytkowników](#)
- 142. [Ustawienia](#)
- 143. [Role](#)
- 144. [Dodaj rolę](#)

- 145. [SMTP](#)
- 146. [Domyślna konfiguracja](#)
- 147. [Basic authentication](#)
- 148. [Modern authentication \(Google\)](#)
- 149. [Modern authentication \(Microsoft 365\)](#)
- 150. [Motyw](#)
- 151. [Aktualizacje](#)
- 152. [Integracje](#)
- 153. [Android Enterprise](#)
- 154. [Android zero-touch](#)
- 155. [Apple Business Manager](#)
- 156. [Apple Push Notification Service](#)
- 157. [Apps and Books](#)
- 158. [Microsoft Entra ID Applications](#)
- 159. [Samsung KME](#)
- 160. [File Manager](#)
- 161. [Changelog](#)
- 162. [Znane problemy](#)
- 163. [Aplikacja mobilna Proget](#)
- 164. [Changelog](#)
- 165. [Znane problemy](#)
- 166. [Aplikacja Proget Notifier](#)
- 167. [Changelog](#)
- 168. [Aplikacja Proget File Manager](#)
- 169. [Changelog](#)
- 170. [Aplikacja Proget Remote](#)
- 171. [Changelog](#)
- 172. [Aplikacja Proget Geofencing](#)
- 173. [Changelog](#)
- 174. [Aplikacja Proget Backup](#)
- 175. [Changelog](#)
- 176. [Aplikacja Proget File Sharing](#)
- 177. [Changelog](#)
- 178. [Aplikacja Proget OpenVPN](#)
- 179. [Changelog](#)
- 180. [FAQ](#)

Ważne informacje

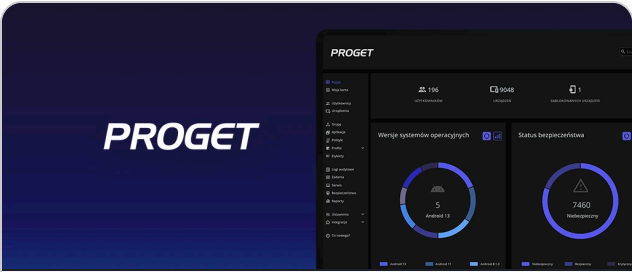
✓ **Konsola Proget**
Wersja 2.20.4

✓ **Aplikacja mobilna Proget**
Wersja 2.20.3

✓ **Proget Notifier**
Wersja 1.0.0

✓ **Proget File Manager**
Wersja 0.1.1

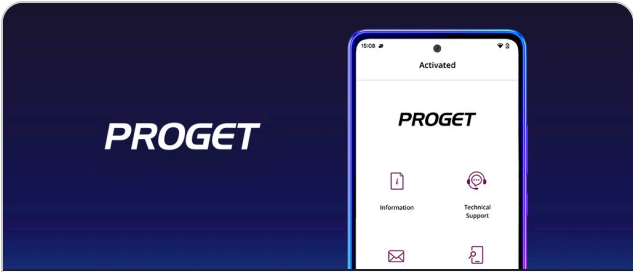
Aplikacje



PROGET

KONSOLA PROGET

→



PROGET

APLIKACJA MOBILNA PROGET

→



PROGET NOTIFIER

PROGET NOTIFIER **NOWOŚĆ**

→

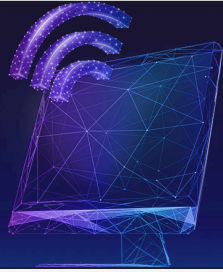


PROGET FILE MANAGER

PROGET FILE MANAGER **NOWOŚĆ**

→

PROGET
REMOTE



PROGET REMOTE



PROGET
GEOFENCING



PROGET GEOFENCING



PROGET
BACKUP



PROGET BACKUP



PROGET
FILE SHARING



PROGET FILE SHARING



PROGET
OPENVPN

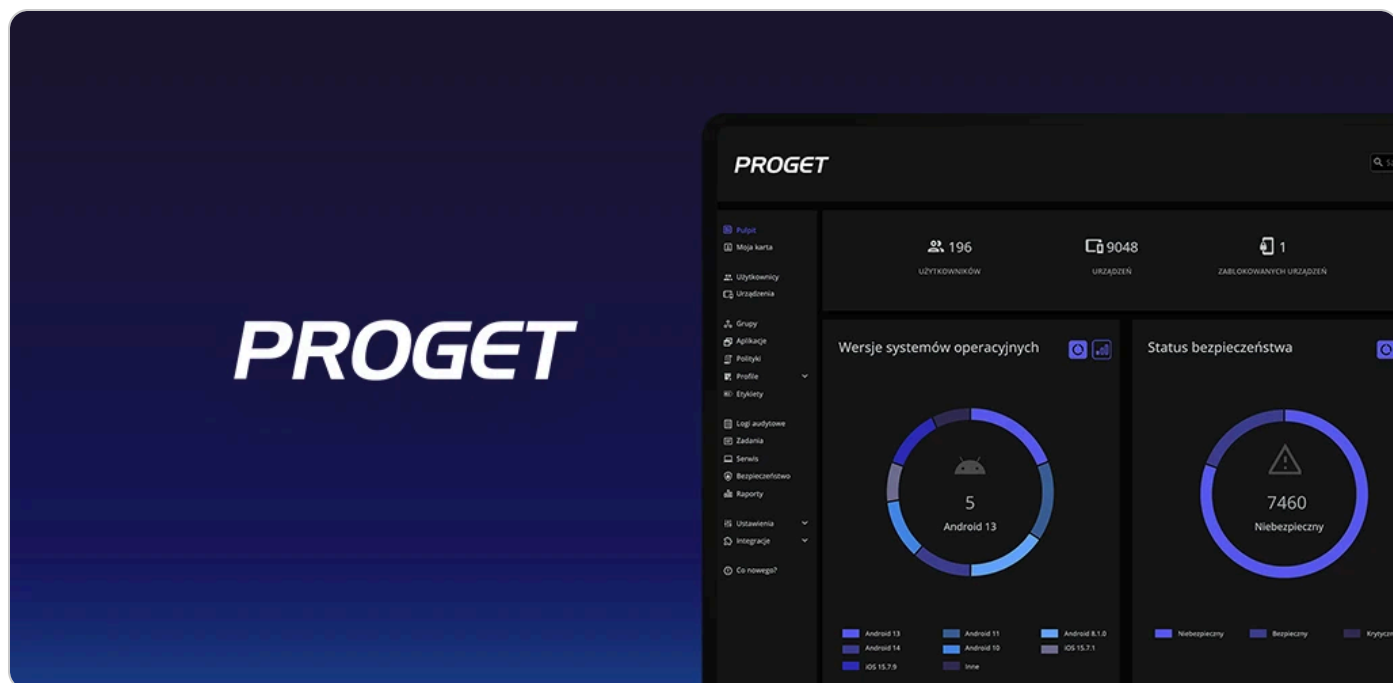


PROGET OPENVPN



Konsola Proget

Zaktualizowano: 13 lut 2025



Przewodnik administratora



Changelog



Znane problemy

Przewodnik Administratora

Zaktualizowano: 16 lip 2026

Przewodnik administratora zawiera informacje o konsoli administratora, które pomogą ci zapoznać się z naszym systemem. Znajdziesz tu opis naszego systemu i jego funkcji, które pomogą Ci rozpocząć korzystanie z naszego produktu.



Logowanie

Logowanie do konsoli w trybie domenowym, lokalnym lub Microsoft...



Pulpit

Przegląd użytkowników, urządzeń, powiadomień i lokalizacji urządzeń



Moja Karta

Dane użytkownika, przypisane urządzenia i dostępne akcje



Użytkownicy

Zarządzanie użytkownikami i dodawanie ich z Entra ID, LDAP lub...



Aktywacje

Aktywacja urządzeń ręczna, automatyczna, z szablonów i własną...



Urządzenia

Tabela urządzeń aktywowanych na serwerze wraz ze szczegółami



Grupy

Grupy do przypisywania polityk, profili i aplikacji wielu urządzeniom



Aplikacje

Tabela aplikacji dostępnych na danym serwerze



Polityki

Ograniczanie funkcji urządzeń: hasła, aparat, usługi Google



Profile

Konfiguracja poczty, lokalizacji, reguł aplikacji, dokumentów i kopii...



Etykiety

Etykiety grup i użytkowników do przypisywania urządzeń



Logi audytowe

Zbieranie i przeglądanie zdarzeń zachodzących na serwerze



Zadania

Zadania wysyłane do urządzeń przez użytkowników lub system



Serwis

Dane o urządzeniach kiedykolwiek aktywowanych na serwerze



Bezpieczeństwo

Tabela zdarzeń bezpieczeństwa zarejestrowanych na urządzeniach



Raporty

Konfiguracja i generowanie raportów o urządzeniach w systemie



Ustawienia

Kontrola dostępu, LDAP, SMTP, certyfikaty, role i inne ustawienia



Integracje

Integracje z Android Enterprise, Apple Business Manager, Entra ID i innymi



File Manager

Zdalne zarządzanie plikami na urządzeniach iOS i Android

Logowanie

Zaktualizowano: 17 gru 2025

Strona logowania umożliwia zalogowanie się do konsoli Proget przy użyciu trybu domeny, lokalnego lub Microsoft Entra ID.

Sign in



EN 

Login mode: ☒ Domain ☐ Local ☐ Microsoft Entra ID

 Domain\Username

 Password 

Sign in

1 Logowanie domenowe

- Wpisz nazwę użytkownika i hasło domeny
- Potwierdź przyciskiem 'Zaloguj się'
- Aby ta opcja działała, LDAP musi być dodany i poprawnie skonfigurowany w konsoli Proget

2 Logowanie lokalne

- Wpisz lokalną nazwę użytkownika lub adres email oraz hasło
- Potwierdź przyciskiem 'Zaloguj się'
- Jeśli zapomniałeś hasła, możesz skorzystać z przycisku 'Zapomniałeś hasła?', a otrzymasz link do zresetowania hasła przez wiadomość email

3 Logowanie Microsoft Entra ID

- Po kliknięciu przycisku 'Microsoft Entra ID' zostaniesz przeniesiony na stronę Microsoft, gdzie możesz zalogować się na konto Microsoft
- Następnie zostaniesz automatycznie zalogowany do konsoli Proget

- Aby ta opcja działała, w ustawieniach Microsoft Entra ID należy włączyć opcję logowania za pomocą usługi Microsoft Entra ID

4

Pomoc

4.1 Przewodnik administratora

- Po kliknięciu przycisku 'Zobacz przewodnik', zostaniesz przeniesiony do dokumentacji Proget, gdzie znajdziesz informacje o naszym systemie (np. FAQ, znane problemy, czy dziennik zmian)

4.2 Baza wiedzy

- Po kliknięciu przycisku 'Przejdź do serwisu', zostaniesz przeniesiony do strony Proget, gdzie znajdziesz informacje na temat całego systemu

4.3 Propozycje

- Po kliknięciu przycisku 'Zgłoś swoją sugestię' masz możliwość przesłania uwag dotyczących istniejących funkcjonalności lub zaproponowania nowych rozwiązań
- Adres email do działu rozwoju produktut

4.4 Wsparcie

- Po kliknięciu przycisku 'Zgłoś problem', zostaniesz przeniesiony do strony Proget, gdzie będziesz mógł wysłać ticket z danym problemem do działu wsparcia
- Adres email do działu wsparcia Proget

4.5 Sprzedaż

- Adres email do działu sprzedaży Proget

4.6 Professional

- Po kliknięciu przycisku 'Sprawdź ofertę', zostaniesz przeniesiony do sklepu Proget, gdzie możesz znaleźć i kupić nasze dodatkowe usługi

Pulpit

Zaktualizowano: 3 gru 2024

Zakładka Pulpit pokazuje liczbę użytkowników, urządzeń i powiadomień na danym serwerze. Można tu znaleźć informacje o urządzeniach, takie jak: wersja systemu operacyjnego, ostatni kontakt z urządzeniem i stan zabezpieczeń. Jeśli jakiegokolwiek urządzenie z konsoli pobrało lokalizację, zostanie ona wyświetlona na mapie.

Search

2

USERS

1

DEVICES

0

BLOCKED DEVICES

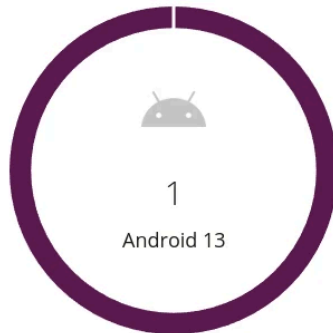
2938

NOTIFICATIONS

0

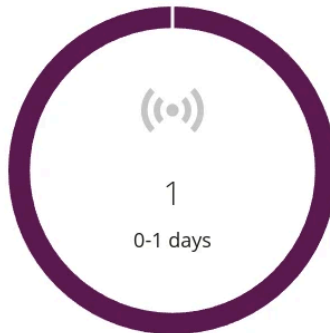
OUT OF COMPLIANCE

Operating system versions



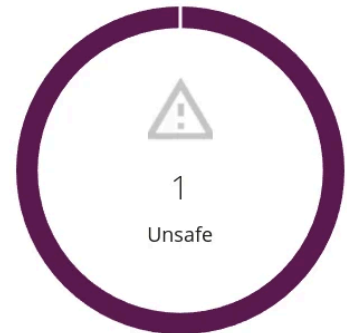
Android 13

Last contact with the device



0-1 days

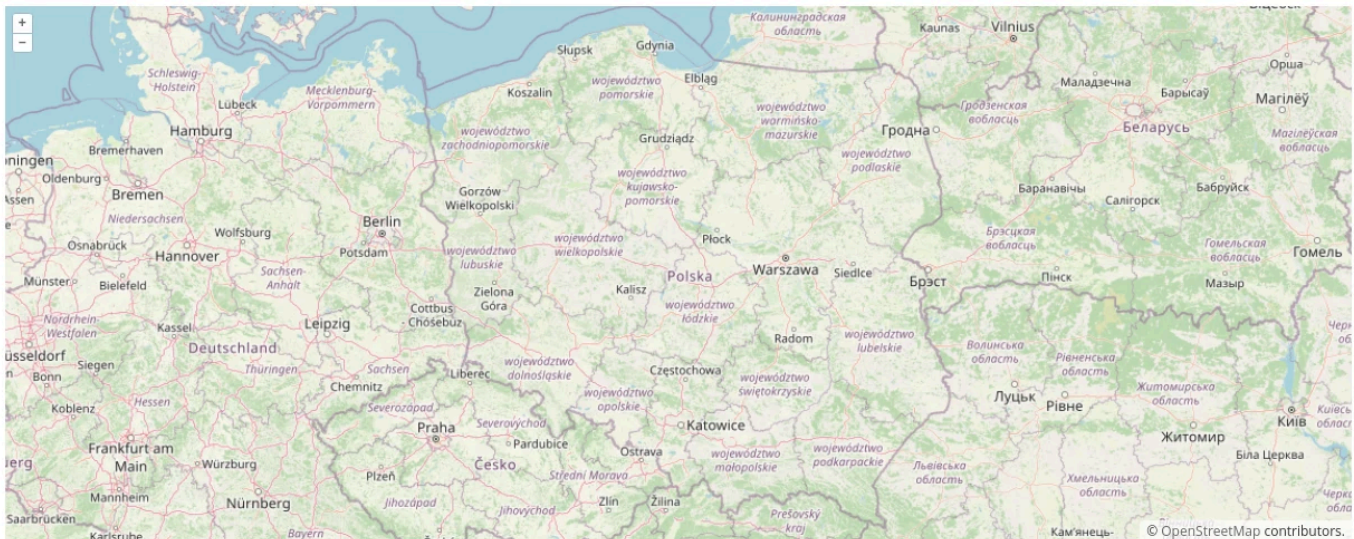
Security status



Unsafe

Safe

Location of devices



1

Szukaj

- Tutaj możesz wyszukiwać wszystko, co zostało utworzone lub dodane do konsoli, np. profile, zasady, użytkowników, urządzenia.

2 Użytkownicy

- Liczba użytkowników dodanych do konsoli Proget
- Ten przycisk przenosi cię do karty Użytkownicy

3 Urządzenia

- Liczba aktywowanych urządzeń w konsoli Proget
- Ten przycisk przenosi cię do karty Urządzenia

4 Zablokowane urządzenia

- Liczba zablokowanych urządzeń w konsoli Proget
- Ten przycisk przenosi cię do karty Urządzenia i wyświetla zablokowane urządzenia

5 Powiadomienia

- Liczba powiadomień w konsoli Proget
- Ten przycisk przenosi cię do sekcji Powiadomienia

6 Niezgodne urządzenia

- Liczba urządzeń niezgodnych z zasadami w konsoli Proget
- Ten przycisk przenosi cię do karty Bezpieczeństwo

7 Wersje systemu operacyjnego

- Interaktywny wykres zawierający dane na temat wersji systemu operacyjnego
- Możliwość przekształcenia go w wykres słupkowy

8 Ostatni kontakt z urządzeniem

- Interaktywny wykres zawierający dane na temat ostatniego kontaktu z urządzeniami w dniach
- Możliwość przekształcenia go w wykres słupkowy

9 Status bezpieczeństwa

- Interaktywny wykres zawierający dane na temat statusu bezpieczeństwa urządzeń
- Możliwość przekształcenia go w wykres słupkowy

10 Lokalizacja urządzeń

- Jeśli lokalizacja jest odczytywana z urządzeń, są one wyświetlane na tej mapie
- Jeśli nie ma urządzeń z odczytaną lokalizacją, mapa jest wyśrodkowana zgodnie z wybranym krajem w ustawieniach

Moja Karta

Zaktualizowano: 16 lip 2026

Karta Moja karta zawiera informacje o użytkowniku i przypisanych do niego urządzeniach. Ponadto daje możliwość wykonywania działań na użytkowniku i aktywnych urządzeniach.

Example User ...

Generate activation

Show activation

LABELS

userExample Group

EMAIL ADDRESS

exampleuser@domain.com

FIRST NAME AND SURNAME

Example User

USERNAME

exampleuser

FIRST NAME

Example

SURNAME

User

TITLE

None

Devices

Attributes

Certificates

Audit logs

Backups

Settings

Dependency graph

Selected: 0

Deselect all

	MANUFACT...	MODEL	IMEI	SERIAL NUMBER	ALIAS	ACTIVATION TYPE	DEVICE LAST CONT...
☐	APPLE	iPhone 7	202000000000000	202000000000000	-	IOS	2026-05-14 11:38:23
☐	GOOGLE	Pixel XL	UNIDENTIFIED		-	Android	2026-05-14 08:41:24
☐	XIAOMI	24129PN74G	UNIDENTIFIED		-	Android Enterprise Profile Owner	2026-05-14 09:33:30
☐	SAMSUNG	SM-A236B	202100000000000	202100000000000	-	Android Enterprise Device Owner	2026-05-14 11:53:32

1

Akcje użytkownika

- Dostępne akcje użytkownika
 - Generuj aktywacje
 - Wyślij email
 - Nadaj status VIP
 - Zarządzaj etykietami
 - Resetuj uwierzytelnianie dwuetapowe
 - Zmień hasło
 - Generuj PIN
 - Certyfikaty

2

Generuj aktywację

2.1 Szablon aktywacji

- Wybierz dostępny szablon aktywacji z rozwijanej listy
- Dostępne szablony aktywacji dla platformy Android, takie jak:
 - Android Enterprise Device Owner
 - Android Enterprise Profile Owner
 - Android MDM
- Wymagane

2.2 Dodaj szablon aktywacji

- Jeśli nie posiadasz dostępnego szablonu aktywacji, możesz go utworzyć za pomocą tej akcji
- Kliknij w tytuł, aby dowiedzieć się, jak to skonfigurować

2.3 Potrzebujesz pomocy?

- Kliknij, jeśli potrzebujesz pomocy z aktywacją urządzenia lub chcesz dowiedzieć się, co oznacza dana aktywacja

2.4 Generuj aktywację

- Ta akcja pozwala na wygenerowanie aktywacji dla wybranej platformy

2.5 iOS

- Generowanie aktywacji dla urządzeń z systemem iOS

2.6 macOS

- Generowanie aktywacji dla urządzeń z systemem macOS

2.7 Windows

- Generowanie aktywacji dla urządzeń z systemem Windows

3 Pokaż aktywację

- Tutaj możesz wyświetlić wygenerowaną już aktywację

4 Urządzenia

5 Atrybuty

6 Certyfikaty

7 Logi Audytowe

8 Kopie Zapasowe

9 Ustawienia

10 Graf zależności

Urządzenia

Zaktualizowano: 3 cze 2026

W tym miejscu możesz wyświetlić wszystkie urządzenia przypisane do Twojego użytkownika.

Devices

Attributes

Certificates

Audit logs

Backups

Settings

Dependency graph

Selected: 0

Deselect all

☐	MANUFACT...	MODEL	IMEI	SERIAL NUMBER	ALIAS	ACTIVATION TYPE	DEVICE LAST CONT...
☐	SAMSUNG	SM-S906B	UNRECOGNIZED	UNRECOGNIZED	-	Android Enterprise Device Owner	2026-05-14 12:22:33
☐	APPLE	iPhone 7	UNRECOGNIZED	UNRECOGNIZED	-	IOS	2026-05-14 12:12:33
☐	GOOGLE	Pixel XL	UNRECOGNIZED		-	Android	2026-05-14 12:11:16
☐	XIAOMI	24129PN74G	UNRECOGNIZED		-	Android Enterprise Profile Owner	2026-05-14 12:15:55

1 Zresetuj hasło na urządzeniu

- Ta akcja pozwala wysłać polecenie do urządzenia, w celu ustawienia nowego hasła

2 Wyślij wiadomość na urządzenie

- Ta akcja pozwala wysłać wiadomość. Podczas wykonywania tej akcji administrator może wybrać, jak wiadomość będzie wyświetlona na urządzeniu

3 Wyślij wiadomość alarmową na urządzenie

- Ta akcja pozwala wysłać wiadomość alarmową. Podczas wykonywania tej akcji administrator musi ustawić treść wiadomości i może wybrać dodatkowe opcje. Wiadomość alarmowa będzie natychmiast widoczna na urządzeniu z charakterystycznym dźwiękiem, a użytkownik będzie zmuszony do zaakceptowania, że przeczytał wiadomość

4 Wykonaj raport

- Ta akcja pozwala sporządzić raport danych na temat wybranego urządzenia, takie jak:
 - Raport zajętości pamięci masowej
 - Raport zużycia danych komórkowych
 - Raport zużycia danych Wi-Fi
 - Raport użycia aplikacji

5 Eksportuj informacje

- Ta akcja pozwala eksportować dane o wybranym urządzeniu

6 Odśwież urządzenie

- Ta akcja pozwala odświeżyć wybrane urządzenie

7 Usuń urządzenie

- Ta akcja pozwala usunąć urządzenie

8 Lista urządzeń

- Lista urządzeń, które zostały aktywowane w konsoli

Atrybuty

Zaktualizowano: 3 cze 2026

W tym miejscu możesz dostosować widok atrybutów do swoich potrzeb.

Devices

Attributes

Certificates

Audit logs

Backups

Settings

Dependency graph

SHOW	ATTRIBUTE	GLOBAL VARIABLE	VALUE
☒	EMAIL ADDRESS	{User:Email}	exampleuser@domain.com
☐	FIRST NAME AND SURNAME	{User:DisplayName}	Example User
☐	USERNAME	{User:Name}	exampleuser
☐	FIRST NAME	{User:FirstName}	Example
☐	SURNAME	{User:LastName}	User
☐	PRINCIPAL NAME	{User:PrincipalName}	-
☐	DISTINGUISHED NAME	{User:DistinguishedName}	-
☐	COMMON NAME	{User:CommonName}	-
☐	DIRECTORY GROUPS	{User:DirectoryGroups}	-
☐	ORGANIZATION	{User:Organization}	-
☐	COUNTRY	{User:Country}	-
☐	ORGANIZATION UNIT	{User:OrganizationUnit}	-
☐	LOCALITY	{User:Locality}	-
☐	STATE	{User:State}	-
☐	ZIP CODE	{User:ZipCode}	-
☐	ADDRESS	{User:Address}	-
☐	PHONE	{User:Phone}	-
☐	FAX	{User:Fax}	-
☐	MOBILE PHONE	{User:Mobile}	+48333000999
☐	TITLE	{User:Title}	-
☐	CUSTOM ATTRIBUTE 1	{User:CustomAttribute1}	Example value
☐	CUSTOM ATTRIBUTE 2	{User:CustomAttribute2}	Example value
☐	CUSTOM ATTRIBUTE 3	{User:CustomAttribute3}	Example value
☐	CUSTOM ATTRIBUTE 4	{User:CustomAttribute4}	Example value

1 Tabela atrybutów

- Podane atrybuty są generowane na podstawie danych o koncie (lokalnie / LDAP / Microsoft Entra ID)
- Stwórz swój własny atrybut używając niestandardowych atrybutów

Certyfikaty

Zaktualizowano: 3 cze 2026

W tym miejscu możesz zobaczyć certyfikaty, które zostały wykorzystane przez Twojego użytkownika w profilach i konfiguracjach aplikacji.

[Devices](#) [Attributes](#) **[Certificates](#)** [Audit logs](#) [Backups](#) [Settings](#) [Dependency graph](#)

Profile:

Issuer:

Validity: From To

Revoked:

[Reset filters](#) [BASIC](#) [PQL](#)

Selected: 0 | [Deselect all](#)

☐	PROFILE	ISSUER	VALIDITY	REVOKED
> ☐	Certyfikat(Template)	CA	2027-05-14 12:12:30	-

1 Odnów certyfikat

- Ta akcja pozwala odnowić wybrany certyfikat

2 Unieważnij certyfikat

- Ta akcja pozwala unieważnić wybrany certyfikat
- Unieważnienie certyfikatu spowoduje zaprzestanie działania funkcjonalności korzystających z tego certyfikatu
- Wybrana akcja jest nieodwracalna

3 Lista certyfikatów

- Lista certyfikatów, zawierająca główne informacje zawarte w certyfikacie użytkownika

Logi Audytowe

Zaktualizowano: 3 cze 2026

W tym miejscu możesz zobaczyć wszystkie logi związane z Twoim użytkownikiem.

DevicesAttributesCertificatesAudit logsBackupsSettingsDependency graph

Action: Select▼

Status: Select▼

Date of occurrence: From SelectTo Select

+

Reset filtersBASICPQL

ACTION	STATUS	DATE OF OCCURRENCE	PERFORMED ON	DETAILS
user.backup.qr.generate	Success	2026-05-14 12:18:58	Example User (exampleuse...)	Backup QR code generated
user.backup.qr.generate	Success	2026-05-14 12:13:21	Example User (exampleuse...)	Backup QR code generated
user.attribute.update	Success	2026-05-14 12:09:11	Example User (exampleuse...)	User attribute customAttribute4 updated
user.attribute.update	Success	2026-05-14 12:09:08	Example User (exampleuse...)	User attribute customAttribute3 updated
user.attribute.update	Success	2026-05-14 12:09:05	Example User (exampleuse...)	User attribute customAttribute2 updated

1

Lista logów audytowych

- Historia zdarzeń w systemie wygenerowana za pomocą określonych akcji użytkownika, przez:
 - System
 - Użytkownika
 - Urządzenie mobilne

Kopie Zapasowe

Zaktualizowano: 3 cze 2026

W tym miejscu możesz stworzyć i wyświetlić kopie zapasowe Twojego użytkownika.

DevicesAttributesCertificatesAudit logsBackupsSettingsDependency graph

Selected: 0Deselect all

Generate QR code

☐	DEVICE	ID	DATE
☐	SAMSUNG SM-S906B	20bc7219-227f-4629-82e9-eb15c2e67659	2026-05-14 12:22
☐	SM-A236B	-	2026-05-14 12:14

1

Usuń kopie zapasowe

- Ta akcja pozwala usunąć kopie zapasowe

2

Generuj kod QR

- Po kliknięciu na ten przycisk, pojawi się okno z możliwością wybrania, dla którego użytkownika ma zostać wygenerowany kod QR do wykonania kopii zapasowej

3

Lista kopii zapasowych

- Lista kopii zapasowych, które zostały utworzone

Ustawienia

Zaktualizowano: 3 cze 2026

W tym miejscu możesz wyświetlić i edytować podstawowe dane o Twoim użytkowniku, oraz spersonalizować konsolę.

Devices

Attributes

Certificates

Audit logs

Backups

Settings

Dependency graph

* First name:

Example

* Surname:

User

* Email:

exampleuser@domain.com

* Username:

exampleuser

Theme:

Light

Submit

1 Imię

- Imię użytkownika
- Wymagane

2 Nazwisko

- Nazwisko użytkownika
- Wymagane

3 Email

- Email użytkownika
- Wymagane

4 Nazwa użytkownika

- Nazwa użytkownika
- Wymagane

5 Motyw

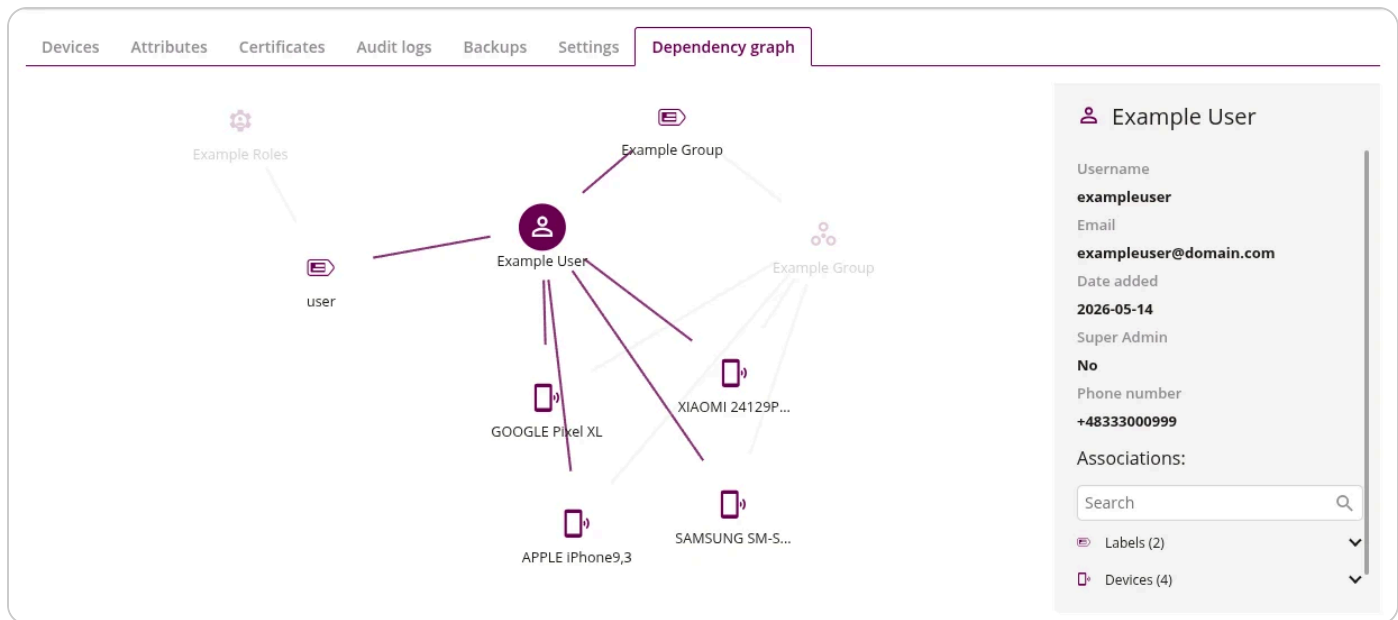
- Typy motywów
 - Jasny
 - Ciemny
 - Automatyczny

Graf zależności

Zaktualizowano: 3 cze 2026

NOWOŚĆ

Zakładka Graf zależności wyświetla interaktywną wizualizację powiązań między kluczowymi elementami systemu, takimi jak etykiety, grupy, użytkownicy, urządzenia, role oraz integracje katalogowe (LDAP/Entra). Pozwala administratorom szybko zrozumieć, jak poszczególne elementy są ze sobą powiązane, bez konieczności przechodzenia między wieloma widokami. Funkcjonalność jest obecnie dostępna wyłącznie dla super administratorów.



1 Graf

- Interaktywny graf pokazujący wybrany element jako centralny węzeł z połączonymi elementami wyświetlanymi wokół niego
- Połączone elementy obejmują urządzenia, grupy, role, etykiety oraz integracje katalogowe
- Kliknij na węzeł, aby wyświetlić jego szczegóły w panelu bocznym
- Węzły z liczbą reprezentują zagregowane elementy - kliknij, aby rozwinąć je do pojedynczych węzłów

2 Panel szczegółów

- Panel boczny wyświetlający szczegółowe informacje o wybranym elemencie, takie jak nazwa użytkownika, email, data dodania, status super admina i numer telefonu
- Sekcja powiązań wyświetla powiązane elementy pogrupowane w akordeony (np. Etykiety, Urządzenia, Grupy, Użytkownicy, Role)
- Użyj pola wyszukiwania, aby filtrować powiązania
- Kliknij na element, aby przejść do jego szczegółowego widoku w systemie

Użytkownicy

Zaktualizowano: 16 lip 2026

Na karcie użytkowników znajdziesz tabelę z informacjami o użytkownikach na danym serwerze. Tutaj możesz wykonywać akcje na wielu lub pojedynczych użytkownikach oraz dodawać użytkowników do systemu z Azure AD, LDAP lub lokalnie.

Email: Start typing...

Username: Start typing...

Type: Select

First name: John

Reset filters

Selected: 0 ...

AddBackups

☐	FIRST NAME	SURNAME	EMAIL	DEVICES	ACTIVATION	DATE ADDED
☐	John	Doe	jdoe@example.com	• SAMSUNG SM-A225F	No activation	2024-08-14

Results: 1 | Page limit: 50

1 Filtrowanie w oknie tekstowym

- Możesz filtrować wyniki, używając słów kluczowych. Wpisz słowo kluczowe, po którym chcesz filtrować, do odpowiedniego pola. Wyniki są filtrowane dynamicznie podczas wpisywania tekstu

2 Wygeneruj aktywację

- Ta akcja pozwala na wygenerowanie aktywacji dla wybranego użytkownika

3 Usuń aktywację

- Ta akcja pozwala na usunięcie wygenerowanej aktywacji dla wybranego użytkownika

4 Wyślij email

- Ta akcja pozwala na wysłanie wiadomości e-mail do wybranego użytkownika

5 Nadaj status VIP

- Ta akcja pozwala na oznaczenie wybranego użytkownika jako VIP

6 Odbierz status VIP

- Ta akcja pozwala na odznaczenie wybranego użytkownika jako VIP

7 Przypisz etykiety

- Ta akcja pozwala na powiązanie wybranego użytkownika z wybraną etykietą

8 Odepnij przypisane etykiety

- Ta akcja pozwala na usunięcie powiązań wybranego użytkownika z wybraną etykietą

9 Resetuj uwierzytelnienie dwuetapowe

- Ta akcja pozwala na zresetowanie uwierzytelniania dwuskładnikowego dla wybranego użytkownika

10 Zablokuj użytkowników

- Ta akcja pozwala na zablokowanie wybranego użytkownika

11 Odblokuj użytkowników

- Ta akcja pozwala na odblokowanie wybranego użytkownika

12 Przydziel funkcję Super Admin

- Ta akcja pozwala na przypisanie funkcji Super Admina wybranemu użytkownikowi

13 Odbierz funkcję Super Admin

- Ta akcja pozwala na odebranie funkcji Super Admina wybranemu użytkownikowi

14 Certyfikaty

- Ta akcja pozwala na dodanie certyfikatów zewnętrznych do użytkownika

15 Zresetuj hasło

- Ta akcja pozwala na zresetowanie hasła wybranego użytkownika lokalnego

16 Zarządzaj użytkownikiem

- Ta akcja pozwala na zarządzanie wybranym użytkownikiem, np. zmianę imienia, nazwiska, adresu email, nazwy użytkownika i zresetowanie hasła

17 Generuj PIN

- Ta akcja pozwala na wygenerowanie kodu PIN dla wybranego użytkownika i jego eksport

18 Eksportuj informacje

- Ta akcja pozwala na eksport danych o wybranym użytkowniku

19 Usuń użytkowników

- Ta akcja pozwala na usunięcie wybranego użytkownika

20 Dodaj użytkownika

- Dostępne opcje dodawania użytkownika do konsoli Proget

20.1 Dodaj użytkownika z Microsoft Entra ID

20.2 Dodaj użytkownika z LDAP

20.3 Dodaj lokalnego użytkownika

21 Kopie zapasowe użytkownika

- Ta akcja przeniesie Cię na stronę, gdzie możesz wysłać kopię zapasową swojego prywatnego urządzenia na serwer

22 Lista użytkowników

- Lista wszystkich użytkowników, którzy zostali dodani do konsoli Proget

Dodawanie użytkownika z Microsoft Entra ID

Zaktualizowano: 3 gru 2024

Dodaj użytkowników do systemu z Microsoft Entra ID. Microsoft Entra ID to usługa w chmurze, która zapewnia administratorom możliwość zarządzania tożsamościami użytkowników końcowych oraz uprawnieniami dostępu.

From Microsoft Entra ID

Labels:

Select

Message language:

Do not send

Selected: 0

Deselect all

Add

Select file

☐	EMAIL	USERNAME	FIRST NAME	SURNAME	PHONE NUMBER	MICROSOFT ENTRA ID
No data available						

Results: 0

Page limit: 50

<<<1>>>

1 Etykiety

- Wybierz etykiety, z którymi chcesz powiązać nowych użytkowników

2 Język wiadomości

- Wybierz język, w którym wiadomość zostanie wysłana do użytkownika
- Aby ta funkcja działała prawidłowo, należy skonfigurować SMTP w zakładce Ustawienia

3 Usun

- Ta akcja pozwala na usunięcie wybranego użytkownika

4 Dodaj użytkownika

4.1 Użytkownik w Microsoft Entra ID

- Wyszukaj użytkownika w Microsoft Entra ID po adresie email

5 Wybierz plik

- Wybierz plik z listą użytkowników, których chcesz dodać do konsoli Proget
- Dozwolony typ pliku: csv

6 Pobierz przykładowy plik CSV

- Ta akcja pozwala na pobranie przykładowego pliku CSV

Dodawanie użytkownika z LDAP

Zaktualizowano: 3 gru 2024

Dodaj użytkowników do systemu z LDAP. LDAP (Lightweight Directory Access Protocol) to protokół oprogramowania umożliwiający każdemu lokalizowanie danych o organizacjach, osobach i innych zasobach, takich jak pliki i urządzenia w sieci.

From LDAP

Labels:

Select

Message language:

Do not send

Selected: 0

Deselect all

Add

Select file

	EMAIL	USERNAME	FIRST NAME	SURNAME	PHONE NUMBER	LDAP
No data available						

Results: 0

Page limit: 50

1 Etykiety

- Wybierz etykiety, z którymi chcesz powiązać nowych użytkowników

2 Język wiadomości

- Wybierz język, w którym wiadomość zostanie wysłana do użytkownika
- Aby ta funkcja działała prawidłowo, należy skonfigurować SMTP w zakładce Ustawienia

3 Usun

- Ta akcja pozwala na usunięcie wybranego użytkownika

4 Dodaj użytkownika

4.1 Użytkownik w LDAP

- Wyszukaj użytkownika w LDAP po adresie email

5 Wybierz plik

- Wybierz plik z listą użytkowników, których chcesz dodać do konsoli Proget
- Dozwolony typ pliku: csv

6 Pobierz przykładowy plik CSV

- Ta akcja pozwala na pobranie przykładowego pliku CSV

Dodawanie użytkownika lokalnego

Zaktualizowano: 3 gru 2024

Dodaj lokalnych użytkowników do systemu.

Local

Labels:

Select

Message language:

Do not send

Selected: 0

Deselect all

Remove duplicates

Add

Select file

☐	FIRST NAME	SURNAME	EMAIL	USERNAME	PHONE NUMBER	ACTIONS
No data available						

Results: 0 | Page limit: 50

<<

<

1

>

>>

1 Etykiety

- Wybierz etykiety, z którymi chcesz powiązać nowych użytkowników

2 Język wiadomości

- Wybierz język, w którym wiadomość zostanie wysłana do użytkownika
- Aby ta funkcja działała prawidłowo, należy skonfigurować SMTP w zakładce Ustawienia

3 Usuń

- Ta akcja pozwala na usunięcie wybranego użytkownika

4 Usuń duplikaty

- Ta akcja pozwala na usunięcie zduplikowanych użytkowników, którzy mają te same dane podczas dodawania

5 Dodaj użytkownika

5.1 Imię

- Wpisz imię nowego użytkownika

5.2 Nazwisko

- Wpisz nazwisko nowego użytkownika

5.3 Email

- Wpisz email nowego użytkownika

5.4 Nazwa użytkownika

- Wpisz nazwę użytkownika nowego użytkownika

5.5 Numer telefonu

- Wpisz numer telefonu nowego użytkownika

6 Wybierz plik

- Wybierz plik z listą użytkowników, których chcesz dodać do konsoli Proget
- Dozwolony typ pliku: csv

7 Pobierz przykładowy plik CSV

- Ta akcja pozwala na pobranie przykładowego pliku CSV

Kopie zapasowe użytkownika

Zaktualizowano: 3 gru 2024

Tutaj będziesz mógł wysłać kopię zapasową swojego prywatnego urządzenia z systemem Android na serwer nawet jeśli nie jest aktywowane w usłudze Proget.

Backups

Created at: From Select To Select

User: Start typing...

Device identifier: Start typing...

Reset filters

Selected: 0

Deselect all

Generate QR code

☐	USER	DEVICE IDENTIFIER	CREATED AT
☐	John Doe	-	2024-08-14 14:16
☐	John Doe	-	2024-08-14 14:16
☐	John Doe	-	2024-08-14 14:15

Results: 3

Page limit: 50

<<

<

1

>

>>

1

Usuń

- Ta akcja pozwala na usunięcie wybranych kopii zapasowych z listy

2

Generuj kod QR

2.1

Wprowadź nazwę użytkownika

- Wpisz nazwę użytkownika, dla którego zostanie wysłana kopia zapasowa na serwer. Następnie kliknij przycisk 'Generuj'
- Wymagane

3 Lista wykonanych kopii zapasowych

- Lista kopii zapasowych wykonanych przez użytkownika

Wygenerowany kod QR kopii zapasowej

1 Kod QR

- Aby wysłać kopię zapasową na serwer, zeskanuj kod QR swoim prywatnym urządzeniem z systemem Android

Aktywacje

Zaktualizowano: 16 lip 2026

Kliknij w wybraną metodę aktywacji, aby zobaczyć szczegóły i dostosować ustawienia.



Aktywacja ręczna

Ręczne wdrożenie urządzenia z wybranym typem aktywacji



Automatyczna rejestracja urządzeń

Automatyzacja i przyspieszenie aktywacji wielu urządzeń



Szablony

Predefiniowane ustawienia do szybkiego tworzenia aktywacji



Własna EULA

Treść własnej umowy wyświetlanej podczas aktywacji urządzenia

Ręczna

Zaktualizowano: 9 paź 2025

Aktywacja ręczna daje możliwość manualnego wdrożenia urządzenia z wybranym typem aktywacji, dla wybranego użytkownika lub bez użytkownika.

Identifier: Start typing...

Created at: From Select To Select

Expiration date: From Select To Select

+

Reset filters

BASICPQL

Selected: 0 | Deselect all

Generate activation

☐	IDENTIFIER	CREATED AT	EXPIRATION DATE	ACTIVATION TYPE	CREATED BY	CREATED FOR
☐	12345-67890	2025-05-21 07:46:59	2025-05-22 07:46:59	Windows	Example Example	Example Example
☐	98765-43210	2025-05-21 07:46:40	2025-05-22 07:46:40	Android Enterprise Device Owner	Example Example	
☐	09876-54321	2025-05-21 07:46:35	2025-05-22 07:46:35	Android Enterprise Profile Owner	Example Example	
☐	56789-01234	2025-05-21 07:46:31	2025-05-22 07:46:31	Android	Example Example	
☐	43210-98765	2025-05-21 07:46:27	2025-05-22 07:46:27	iOS	Example Example	
☐	32109-87654	2025-05-21 07:46:23	2025-05-22 07:46:23	macOS	Example Example	

1

Filtr wygenerowanych aktywacji

- Wyszukaj aktywacje, używając dostępnych filtrów, takich jak:
 - Identyfikator
 - Data utworzenia
 - Data ważności
 - Typ aktywacji
 - Utworzone przez
 - Utworzone dla

2

Pokaż

- Ta akcja pozwala na podgląd wybranej z listy dostępnej aktywacji

3**Usuń**

- Ta akcja pozwala na usunięcie jednej lub więcej wybranych aktywacji
- Ta akcja jest nieodwracalna

4**Generuj aktywację**

4.1 Szablon aktywacji

- Wybierz dostępny szablon aktywacji z rozwijanej listy
- Dostępne szablony aktywacji dla platformy Android, takie jak:
 - Android Enterprise Device Owner
 - Android Enterprise Profile Owner
 - Android MDM
- Wymagane

4.2 Dodaj szablon aktywacji

- Jeśli nie posiadasz dostępnego szablonu aktywacji, możesz go utworzyć za pomocą tej akcji

4.3 Bez użytkownika

- Jeśli ta opcja jest wybrana, aktywacja zostanie wygenerowana bez przypisania do żadnego użytkownika
- Aktywowane urządzenie nie zostanie przypisane do żadnego użytkownika w systemie MDM

4.4 Z użytkownikiem

- Jeśli opcja jest wybrana, podczas generowania aktywacji należy podać użytkownika, do którego zostanie przypisana aktywacja
- Urządzenie po aktywacji zostanie przypisane do tego użytkownika w systemie MDM

4.5 Liczba aktywacji

- Suwak jest dostępny tylko gdy wybrana jest opcja **Bez użytkownika**
- Pozwala zdefiniować liczbę generowanych aktywacji od 1 do 100
- Wymagana jest opcja **Bez użytkownika**

4.6 Potrzebujesz pomocy?

- Kliknij, jeśli potrzebujesz pomocy z aktywacją urządzenia lub chcesz dowiedzieć się, co oznacza dana aktywacja

4.7 Generuj aktywację

- Ta akcja pozwala na wygenerowanie aktywacji z wprowadzonymi ustawieniami

4.8 iOS

- Generowanie aktywacji dla urządzeń z systemem iOS

4.9 macOS

- Generowanie aktywacji dla urządzeń z systemem macOS

4.10 Windows

- Generowanie aktywacji dla urządzeń z systemem Windows

5 List of activations

- Lista wygenerowanych aktywacji, zawierająca główne informacje

Automatyczna

Zaktualizowano: 13 paź 2025

Funkcja automatycznej rejestracji znacznie przyspiesza i usprawnia proces aktywacji wielu urządzeń.

Device auto enrollment

Serial number / IMEI:

Activation type:

User:

Status:

+

Reset filters

Selected: 0 | Deselect all



Add devices

Import CSV

☐	CREATED AT	SERIAL NUMBER / IMEI	INTEGRATION TYPE	ACTIVATION TYPE	USER	ALIAS	POLICY	STATUS	ENROLLED
☐	2024-08-27 11:37:46	20-4000110000000000	Proget	Android Enterprise Device Owner	John Doe			Added	No
☐	2024-08-27 11:37:28	20-4000110000000000	Proget	IOS	John Doe	Example alias		Added	No

Results: 2 | Page limit:



1 Filtrowanie w oknie tekstowym

- Możesz również filtrować wyniki, używając słów kluczowych. Wprowadź słowo kluczowe, które chcesz użyć do filtrowania, w odpowiednim polu. Wyniki są filtrowane dynamicznie podczas wpisywania tekstu.

2 Zaktualizuj rejestrację

- Kliknij przycisk, jeśli chcesz dokonać zmian dla dodanej aktywacji

3 Usuń rejestrację

- Kliknij przycisk, jeśli chcesz usunąć dodaną aktywację

4 Dodaj urządzenia

4.1 Typ wdrożenia

- Wybierz typ wdrożenia:
 - Proget - umożliwia automatyczną rejestrację urządzenia po zainstalowaniu aplikacji
 - KME - umożliwia automatyczną rejestrację urządzenia wraz z instalacją aplikacji. Dostępne tylko na urządzeniach Samsung

4.2 Dodaj urządzenia przez

- Wybierz sposób dodawania urządzenia:
 - IMEI
 - Numer seryjny

4.3 Przypisz szablon Aktywacji

- Ta akcja pozwala na przypisanie szablonu aktywacji dla wybranych urządzeń z listy

4.4 Przypisz politykę

- Ta akcja pozwala na przypisanie polityki dla wybranych urządzeń z listy

4.5 Przypisz akcję po aktywacji

- Ta akcja pozwala na przypisanie reakcji po aktywacji urządzenia w konsoli, takich jak:
 - Brak akcji
 - Odepnij użytkownika od automatycznej rejestracji

4.6 Usuń

- Ta akcja pozwala na usunięcie dodanego urządzenia

4.7 IMEI/Numer seryjny

- Wprowadź numer identyfikacyjny urządzenia

4.8 Użytkownik

- Wprowadź użytkownika, do którego zostanie przypisane dodane urządzenie

4.9 Szablon aktywacji

- Przypisz szablon aktywacji do rejestracji urządzenia

4.10 Polityka

- Przypisz politykę do rejestracji urządzenia

4.11 Akcja po aktywacji

- Przypisz akcję po aktywacji urządzenia

4.12 Alias

- Wprowadź alias dla urządzenia

4.13 Dodaj

- Dodaj nową rejestrację urządzenia

5 Importuj CSV

5.1 Typ wdrożenia

- Wybierz typ wdrożenia:
 - Proget - automatyczna rejestracja urządzenia po zainstalowaniu aplikacji
 - KME - automatyczna rejestracja urządzenia wraz z instalacją aplikacji. Dostępne tylko na urządzeniach Samsung

5.2 Dodaj urządzenia przez

- Wybierz sposób dodawania urządzenia:
 - IMEI
 - Numer seryjny

5.3 Szablon Aktywacji

- Przypisz szablon aktywacji z rozwijanej listy dla wybranych urządzeń

5.4 Polityka

- Przypisz politykę, która będzie obowiązywać urządzenie podczas rejestracji

5.5 Akcja po aktywacji

- Przypisz reakcję po aktywacji urządzenia w konsoli, taką jak:
 - Brak akcji
 - Odepnij użytkownika od automatycznej rejestracji

5.6 Wybierz plik

- Ta akcja pozwala na dodanie pliku w celu importu urządzeń

- Wymagane

5.7 Pobierz przykładowy plik CSV

- Ta akcja pozwala na pobranie przykładowego pliku CSV
- Plik zawiera przykładowy IMEI, email użytkownika, typ rejestracji i alias

6 Lista urządzeń

- Lista urządzeń dodanych do automatycznej rejestracji
- Lista informacji o dodanych urządzeniach i aktualnym statusie

Szablony

Zaktualizowano: 3 cze 2026

Szablony aktywacji pozwalają na szybkie tworzenie aktywacji z predefiniowanymi ustawieniami.

Name:
Type:
Custom EULA:

Reset filters
BASIC PQL

Selected: 0 | Deselect all
Add

☐	NAME	TYPE	CUSTOM EULA	AUTO ENROLLMENT	MICROSOFT ENTRA ID	LDAP
☐	Custom Template - Android	Android	Example Eula	0	0	0
☐	Custom Template - Android Enterprise Device Owner	Android Enterprise Device Owner	-	0	0	0
☐	Custom Template - Android Enterprise Profile Owner	Android Enterprise Profile Owner	-	0	0	0
☐	Custom Template - iOS	iOS	-	0	0	0
☐	Custom Template - macOS	macOS	-	0	0	0
☐	Custom Template - Windows	Windows	-	0	0	0

1 Filtr utworzonych szablonów

- Wyszukaj szablon, używając dostępnych filtrów, takich jak:
 - Nazwa
 - Typ
 - Własna EULA

2 Kopiuj

- Ta akcja pozwala na duplikowanie już istniejącego szablonu w konsoli
- Nie można skopiować szablonu o tej samej nazwie

3 Edytuj

- Ta akcja pozwala na edycję wybranego szablonu z listy

4 Usuń

- Ta akcja pozwala na usunięcie wybranego szablonu z listy
- Możliwe jest usunięcie wielu pozycji jednocześnie

5 Dodaj

- Ta akcja pozwala na dodanie nowego, własnego szablonu

6 Lista szablonów

- Lista wszystkich utworzonych szablonów wraz z ich parametrami

Konfiguracja szablonu

Zaktualizowano: 16 lip 2026

Tutaj możesz skonfigurować szablon aktywacyjny według własnych potrzeb, wybierając odpowiedni typ aktywacji dla urządzeń z systemem Android, Apple iOS, Apple macOS lub Windows

- Android Enterprise Profile Owner
- Android
- iOS
- macOS
- Windows

3 Ustawienia zabezpieczeń

3.1 Pozwól na aktywację na wielu urządzeniach

- Jeśli zaznaczone, funkcja pozwala na aktywację wielu urządzeń w systemie Proget. Jeśli odznaczone, aktywacja zostanie usunięta po wdrożeniu pierwszego urządzenia

3.2 Ogranicz liczbę dni dla aktywacji

- Jeśli zaznaczone, możesz określić liczbę dni ważności aktywacji

3.3 Ilość dni na aktywację

- Wybierz liczbę dni, przez które aktywacja będzie ważna

3.4 Ilość prób aktywacji

- Wybierz, ile razy wygenerowana aktywacja może zostać użyta

3.5 Długość generowanego identyfikatora

- Wybierz długość identyfikatora, który zostanie wygenerowany podczas aktywacji

3.6 Długość generowanego hasła

- Wybierz długość hasła, które zostanie wygenerowane podczas aktywacji

4 Ustawienia wiadomości aktywacyjnej

4.1 Dostarcz aktywację przez email

- Wybierz sposób dostarczenia aktywacji przez email, np.:
 - Nie wysyłaj
 - Zapytaj podczas generowania aktywacji
 - Wyślij
- Aby ta funkcja działała poprawnie, należy najpierw skonfigurować SMTP w zakładce Ustawienia.

4.2 Temat

- Wprowadź temat wiadomości email z aktywacją
- Maksymalna długość tekstu to 255 znaków
- Wymagane, jeśli nie wybrano opcji **Nie wysyłaj**

4.3 Wiadomość

- Wprowadź treść wiadomości email z aktywacją
- Wymagane, jeśli nie wybrano opcji **Nie wysyłaj**

5 Ustawienia na urządzeniach z systemem Android

5.1 Własna EULA

- Jeśli została utworzona, możesz ustawić własną EULA dla tej aktywacji
 - Aby dowiedzieć się, jak utworzyć własną EULA, kliknij w tytuł

5.2 Pozostaw wszystkie aplikacje systemowe włączone

- Jeśli zaznaczone, funkcja pozwala na pozostawianie włączonych aplikacji systemowych na urządzeniu dodawanym do systemu Proget
- Funkcja dostępna w Android Enterprise Profile Owner i Android Enterprise Device Owner przy wdrożeniu za pomocą Enterprise QR kodów

5.3 Dodaj połączenie z siecią Wi-Fi do kodu QR

- Jeśli zaznaczone, urządzenie automatycznie połączy się z określoną siecią
- Kod QR będzie zawierał niezaszyfrowane hasło do sieci Wi-Fi

5.4 SSID

- Wprowadź nazwę identyfikującą sieć bezprzewodową
- Wymagane

5.5 Sieć ukryta

- Wymagane, jeśli sieć, dla której przygotowywana jest konfiguracja, ukrywa identyfikator SSID

5.6 Typ zabezpieczeń

- Jedna z opcji:
 - None
 - WPA Personal
- Jeśli wybrano **None**, sieć będzie niezabezpieczona

- Jeśli wybrano **Personal WPA**, uwierzytelnianie użytkownika odbywa się za pomocą klucza współdzielonego

5.7 Klucz wstępny

- Wpisz klucz wstępny, aby uwierzytelnić się w sieci Wi-Fi
- Dostępne, jeśli wybrano **Typ zabezpieczeń: Personal WPA**

6 Ustawienia na urządzeniach z systemem iOS oraz macOS

6.1 Własna EULA

- Jeśli została utworzona, możesz ustawić własną umowę EULA dla tej aktywacji
 - Aby dowiedzieć się, jak utworzyć własną EULA, kliknij w tytuł

6.2 Włącz zarządzanie deklaratywne

- Jeśli zaznaczone, użytkownik oraz administrator zyskuje dodatkowe funkcje, takie jak:
 - Korzyści dla organizacji:
 - Łatwiejsze egzekwowanie aktualizacji oprogramowania
 - Dynamiczne i skalowalne zarządzanie
 - Zwiększone bezpieczeństwo danych poprzez zarządzanie politykami i ustawieniami
 - Korzyści dla użytkownika końcowego:
 - Płynniejsze działanie systemu operacyjnego urządzenia
 - Urządzenia zachowują niezależność od sieci, samodzielnie utrzymują wymagany stan i automatycznie konfiguruje się po odzyskaniu połączenia
- Wymagany system iOS w wersji 16 lub nowszej
- Wymagany system macOS w wersji 13 lub nowszej

6.3 Pokaż ikonę Proget Store

- Jeśli zaznaczone, ikona Proget Store zostanie wyświetlona na urządzeniu

6.4 Pozwól na wyczyszczenie danych urządzenia

- Jeśli zaznaczone, użytkownik będzie mógł wyczyścić dane swojego nienadzorowanego urządzenia
- Nie dotyczy urządzeń wdrożonych przez ABM

6.5 Pozwól na inspekcję zainstalowanych aplikacji

- Jeśli zaznaczone, aplikacje zainstalowane na nienadzorowanym urządzeniu będą widoczne dla administratora konsoli Proget
- Nie dotyczy urządzeń wdrożonych przez ABM

Własna EULA

Zaktualizowano: 3 cze 2026

Treść umowy, która będzie wyświetlana użytkownikowi podczas procesu aktywacji urządzenia.
Użytkownik musi ją zaakceptować, aby zakończyć rejestrację urządzenia.

Name:

Reset filters

BASIC PQL

Selected: 0 | Deselect all



Add 

☐	NAME ▾	ACTIVATIONS	ACTIVATION TEMPLATES	DEVICES
☐	Example Eula	1	2	1

1 Filtr utworzonych Custom EULA

- Wyszukaj własnej EULA, używając dostępnych filtrów, takich jak:
 - Nazwa

2 Kopiuj

- Ta akcja pozwala na duplikowanie już istniejącej EULA w konsoli
- Nie można skopiować EULA o tej samej nazwie

3 Edytuj

- Ta akcja pozwala na edycję wybranej EULA z listy

4 Usun

- Ta akcja pozwala na usunięcie wybranej EULA z listy
- Możliwe jest usunięcie wielu pozycji jednocześnie

5 Dodaj

- Ta akcja pozwala na dodanie nowej, własnej EULA

6 Lista własnych EULA

- Lista wszystkich utworzonych EULA wraz z ich parametrami

Konfiguracja EULA

Zaktualizowano: 3 cze 2026

Tutaj możesz zdefiniować własną umowę EULA, określając jej nazwę, tytuł oraz treść, która zostanie wyświetlona na urządzeniu podczas aktywacji.

* Name:

Example Eula

* Title:

Example Title

* Content:

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

(577 / 200000 chars)

1 Nazwa

- Wprowadź nazwę własnej EULA
- Maksymalna długość tekstu to 255

2 Tytuł

- Wprowadź tytuł EULA
- Maksymalna długość tekstu to 64

3 Treść

- Wprowadź treść EULA
- Maksymalna długość tekstu to 200000

Urządzenia

Zaktualizowano: 16 lip 2026

Zakładka urządzenia pokazuje tabelę z informacjami o urządzeniach aktywowanych na danym serwerze.

IMEI:

Serial number:

User:

Security status: Select

[Reset filters](#)
BASIC PQL

Selected: 0

Generate activation

☐ MANUFACTURER ▾	MODEL ▾	SYSTEM VERSION ▾	ACTIVATION TYPE ▲
☐ SAMSUNG	SM-A236B	Android 14	Android Enterprise Device Owner
☐ XIAOMI	24129PN74G	Android 16	Android Enterprise Profile Owner
☐ GOOGLE	Pixel XL	Android 10	Android
☐ APPLE	iPhone 7	iOS 15.8.7	iOS
☐ APPLE	Mac14,7	macOS 26.2	macOS
☐ Innotek GmbH	VirtualBox	Windows 10 Enterprise Evaluation	Windows

1 Filtrowanie w oknie tekstowym

- Możesz również filtrować wyniki, używając słów kluczowych. Wpisz słowo kluczowe, które chcesz użyć do filtrowania, w odpowiednie pole. Wyniki są filtrowane dynamicznie podczas wpisywania tekstu.

2 Szybkie akcje

2.1 Dodaj powiązanie z profilem Apple Business Manager

- Ta akcja pozwala przypisać wybrane urządzenie do profilu Apple Business Manager

2.2 Usuń powiązanie z profilem Apple Business Manager

- Ta akcja pozwala usunąć wybrane urządzenie z profilu Apple Business Manager

2.3 Wyślij Custom Apple Command

- Ta akcja pozwala na wysłanie Custom Apple Command do urządzenia

2.4 Włącz zarządzanie deklaratywne

- Ta akcja pozwala na włączenie zarządzania deklaratywnego na urządzeniu iOS lub macOS

2.5 Dodaj konto Android Enterprise

- Ta akcja pozwala dodać konto Android Enterprise do wybranego urządzenia

2.6 Usuń konto Android Enterprise

NOWOŚĆ

- Ta akcja pozwala na usunięcie konta Android Enterprise na wybranym urządzeniu

2.7 Sprawdź status konta Android Enterprise

- Ta akcja pozwala sprawdzić status konta Android Enterprise na wybranym urządzeniu

2.8 Przypisz użytkownika

- Ta akcja pozwala przypisać użytkownika do wybranego urządzenia

2.9 Odepnij użytkownika

- Ta akcja pozwala usunąć przypisanie użytkownika z wybranego urządzenia

2.10 Zablokuj ekran urządzenia

- Ta akcja pozwala zablokować ekran na wybranym urządzeniu

2.11 Włącz Activation Lock

- Ta akcja pozwala włączyć blokadę aktywacji na wybranych urządzeniach

2.12 Wyłącz Activation Lock

- Ta akcja pozwala wyłączyć blokadę aktywacji na wybranych urządzeniach

2.13 Zresetuj hasło urządzenia

- Ta akcja pozwala zresetować hasło na wybranym urządzeniu

2.14 Wyślij wiadomość na urządzenie

- Ta akcja pozwala wysłać wiadomość do wybranego urządzenia
- Podstawowa obsługa formatowania tekstu (m.in. pogrubienie, kursywa) oraz klikane linki do:

NOWOŚĆ

- stron WWW '(https://...)'
- połączeń telefonicznych '(tel://...)'
- konkretnych aplikacji w postaci deep linków '(myapp://...)'

2.15 Wyślij wiadomość alarmową na urządzenie

- Ta akcja pozwala wysłać wiadomość alarmową do wybranego urządzenia

2.16 Wykonaj raport

- Ta akcja pozwala sporządzić raport danych na temat wybranego urządzenia, takie jak:
 - Raport zajętości pamięci masowej
 - Raport zużycia danych komórkowych
 - Raport zużycia danych Wi-Fi
 - Raport użycia aplikacji

2.17 Eksportuj informacje

- Ta akcja pozwala eksportować dane o wybranym urządzeniu

2.18 Odśwież urządzenie

- Ta akcja pozwala odświeżyć wybrane urządzenie

2.19 Zaktualizuj aplikacje

- Ta akcja pozwala zaktualizować wszystkie aplikacje na wybranych urządzeniach

2.20 Ustaw własność

- Ta akcja pozwala ustawić status własności urządzenia, takie jak:
 - Prywatne
 - Służbowe
 - COPE

2.21 Usuń urządzenie

- Ta akcja pozwala usunąć urządzenie

3 Generuj aktywację

- Po kliknięciu przycisku zostaniesz przeniesiony do strony ręcznej aktywacji, gdzie będziesz mógł wygenerować aktywację

4 Tabela urządzeń

4.1 Aktywacja Android Enterprise Device Owner

4.2 Aktywacja Android Enterprise Profile Owner (COPE)

4.3 Aktywacja Androida

4.4 Aktywacja iOS (Tryb nadzorowany)

4.5 Aktywacja macOS

4.6 Aktywacja Windows

Aktywacje

Zaktualizowano: 16 lip 2026

Kliknij na aktywację, która Cię interesuje, aby uzyskać szczegóły.



Aktywacja Android Enterprise Device Owner

Wymaga urządzenia zresetowanego do ustawień fabrycznych



Aktywacja Android Enterprise Profile Owner (COPE)

Rozszerzone zarządzanie dla urządzeń Android 11+ po resecie



Aktywacja Android

Najprostszy typ aktywacji z podstawowym zdalnym zarządzaniem



Aktywacja iOS (Tryb nadzorowany)

Rozszerzona kontrola urządzenia, wymaga konfiguracji ABM



Aktywacja macOS

Aktywacja i konfiguracja ograniczeń na urządzeniach macOS



Aktywacja Windows

Aktywacja i konfiguracja ograniczeń na urządzeniach Windows

Android Enterprise Device Owner

Zaktualizowano: 28 maj 2026

Aktywacja Android Enterprise Device Owner możliwa jest tylko na urządzeniach, które zostały zresetowane do ustawień fabrycznych.

XIAOMI 24129PN74G

User:

Example User

Activation type:

Android Enterprise Device Owner

Alias:

Enter device alias

Last contact:

2026-05-22 10:29:06

Battery level: 54%

Health: Good

Internal storage: 3.6%

Total: 461.33 GiB (495.35 GB) Free: 444.70 GiB (477.50 GB)

External storage:

No external memory card

RAM: 47.67%

Total: 10.84 GiB (11.64 GB) Free: 5.67 GiB (6.09 GB)

Generate service password

Details

Policy

Profiles

Applications

Location

Backups

Audit logs

Tasks

Dependency graph

File Manager

Reports

Export

...

Technical data

Manufacturer:

XIAOMI

Model:

24129PN74G

OS:

Android 16 (36)

Serial number:

40a13aef

IMEI 1:

86408870177764

IMEI 2:

86408870177762

Proget ID:

523 132

Activation date:

2026-05-22 10:19:22

App version:

2.20.1 (1201)

Patch version:

BP2A.250605.031.A3

Bootloader version:

unknown

Security patch:

2026-04-01

System update status:

No info

CPU:

QTI SM8750 (arm64-v8a)

Connection type:

Wi-Fi

IP:

192.168.0.101

Wi-Fi MAC:

8c:30:88:42:a3:98

Wi-Fi SSID:

ProgetWiFi

Roaming:

✗

Data encryption:

✓

Access to device usage data:

✓

Android Enterprise status:

Registered

Google Play services:

✓

Remote password change on the device:

✓

Lost mode enabled:

✗

Access to background activity:

✓

Access to Wi-Fi management:

✓

Runtime permissions:

✓ Telephone ✓ SMS ✓ Call log ...

Groups

Example Group

Security

✗ 0

⚠ 0

✓ 2

ℹ 0

Root status 2026-05-22 10:19:22

Play Integrity verification status 2026-05-22 10:19:25

1 Informacje ogólne

1.1 Wprowadź alias urządzenia

- Ta akcja pozwala ustawić alias urządzenia. Alias może pomóc w identyfikacji urządzenia

1.2 Odśwież urządzenie

- Ta akcja pozwala wysłać polecenie odświeżenia urządzenia w celu aktualizacji informacji i statusu urządzenia

1.3 Generuj hasło serwisowe

- Ta akcja pozwala wygenerować hasło serwisowe dla urządzenia, na którym nałożono tryb Utracony

2 Szybkie akcje

2.1 Zablokuj urządzenie

- Ta akcja pozwala wysłać polecenie zablokowania urządzenia. Gdy urządzenie jest zablokowane, użytkownik może dzwonić tylko do administratora lub na numer alarmowy, który został wprowadzony podczas akcji "Zablokuj urządzenie"

2.2 Odblokuj urządzenie

- Ta akcja pozwala wysłać polecenie odblokowania urządzenia

2.3 Pulpit zdalny

- Aby użyć tej akcji, musisz mieć zainstalowaną aplikację Proget Remote na swoim urządzeniu. Proget Remote to aplikacja, która pozwala na zdalny dostęp do ekranu urządzenia Android z serwera Proget

2.4 Resetuj hasło

- Ta akcja pozwala wysłać polecenie do urządzenia, które spowoduje żądanie zresetowania hasła

2.5 Zmień hasło

- Ta akcja pozwala wysłać polecenie do urządzenia w celu ustawienia nowego hasła na urządzeniu

2.6 Wyczyść dane urządzenia

- Ta akcja pozwala przywrócić ustawienia fabryczne

2.7 Wyczyść dane służbowe

- Ta akcja pozwala na usunięcie danych firmowych. Po wykonaniu tej akcji urządzenie zarejestrowane w konsoli Proget zostanie usunięte, a dalsze zarządzanie tym urządzeniem nie będzie możliwe. Aplikacje Proget nadal będą widoczne, a kolejna rejestracja w konsoli Proget będzie możliwa

2.8 Zablokuj ekran urządzenia

- Ta akcja pozwala wysłać polecenie do urządzenia, które zablokuje ekran urządzenia

2.9 Wyślij wiadomość

- Ta akcja pozwala wysłać wiadomość. Podczas wykonywania tej akcji administrator może wybrać, jak wiadomość będzie wyświetlona na urządzeniu

2.10 Wiadomość alarmowa

- Ta akcja pozwala wysłać wiadomość alarmową. Podczas wykonywania tej akcji administrator musi ustawić treść wiadomości i może wybrać dodatkowe opcje. Wiadomość alarmowa będzie natychmiast widoczna na urządzeniu z charakterystycznym dźwiękiem, a użytkownik będzie zmuszony do zaakceptowania, że przeczytał wiadomość

2.11 Przekieruj połączenia

- Ta akcja pozwala wysłać polecenie przekierowania połączeń telefonicznych na podany numer telefonu

2.12 Usuń przekierowanie połączeń

- Ta akcja pozwala wysłać polecenie usunięcia numeru, na który były przekierowane połączenia

2.13 Odśwież urządzenie

- Ta akcja pozwala wysłać polecenie odświeżenia urządzenia w celu aktualizacji informacji i statusu urządzenia

2.14 Restartuj urządzenie

- Ta akcja pozwala wysłać polecenie do urządzenia w celu jego ponownego uruchomienia

2.15 Włącz tryb kiosk

- Ta akcja pozwala wysłać polecenie do urządzenia w celu włączenia profilu kiosku. Akcja jest dostępna, gdy profil kiosku jest dodany do urządzenia

2.16 Wyłącz tryb kiosk

- Ta akcja pozwala wysłać polecenie do urządzenia w celu wyłączenia profilu kiosku. Akcja jest dostępna, gdy profil kiosku jest dodany do urządzenia

2.17 Zweryfikuj urządzenie

- Ta akcja pozwala na weryfikację zgodności urządzenia z polityką Play Integrity

2.18 Wygeneruj dziennik zdarzeń

- Ta akcja pozwala wygenerować i wysłać logi audytowe na serwer Proget

3 Tabele

3.1 Podstawowe

3.2 Polityka

3.3 Profile

3.4 Aplikacje

3.5 Lokalizacja

3.6 Kopie zapasowe

3.7 Logi audytowe

3.8 Zadania

3.9 Graf zależności

3.10 File Manager

3.11 Raporty

3.12 Eksport

3.13 Konta użytkownika

3.14 Raporty o błędach systemowych

3.15 Zdjęcia z blokady

3.16 Użytkownicy

Hasło serwisowe

Zaktualizowano: 9 cze 2026

NOWOŚĆ

Panel Hasło serwisowe umożliwia administratorowi wygenerowanie awaryjnego hasła serwisowego dla urządzenia. Hasło jest powiązane z konkretnym urządzeniem i ma określony czas ważności (domyślnie 24 godziny, minimalnie 5 minut, maksymalnie 30 dni). Działa nawet gdy urządzenie jest w trybie Lost Mode, Kiosku, nie ma połączenia z internetem lub lokalna baza danych jest uszkodzona. Po użyciu urządzenie wchodzi w 60-minutowe okno uprzywilejowanego działania, po czym wraca do stanu wymaganego przez polityki. Hasło można wpisać ręcznie lub zeskanować jako kod QR na urządzeniu.



Service password

* Select actions: ⓘ

- ☐ Unblock device
- ☐ Disable Kiosk
- ☐ Remove network restrictions ⓘ
- ☐ Allow developer options
- ☐ Allow deactivation
- ☐ Allow factory reset
- ☐ Emergency Database Reset ⓘ
- ☐ Set Password ⓘ

* Service password expiration date (on device):

2026-05-07 10:23



Time to expire: in about 24 hours

- ☒ Generate QR code
- ☒ Send service password via email

* Email:

example@domain.com

Message language:

English



Cancel

Generate

1 Odblokuj urządzenie

- Jeśli zaznaczone, hasło serwisowe odblokuje urządzenie z trybu Lost Mode

2 Wyłącz Kiosk

- Jeśli zaznaczone, hasło serwisowe wyjdzie z trybu Kiosk na urządzeniu

3 Usuń ograniczenia sieciowe

- Jeśli zaznaczone, hasło serwisowe tymczasowo usunie ograniczenia sieciowe na urządzeniu
 - Jeśli zaznaczone, hasło serwisowe tymczasowo usunie ograniczenia sieciowe na urządzeniu
 - Akcja ściąga restrykcje nałożone przez polityki związane z siecią:
 - Pozwalaj na zmianę ustawień sieci komórkowej

- Pozwalaj używać danych komórkowych podczas roamingu
- Pozwalaj na konfigurację tetheringu oraz mobilnego punktu dostępu
- Pozwalaj edytować konfiguracje Wi-Fi
- Określ ustawienia konfiguracji podtrzymania Wi-Fi po uśpieniu (Zawsze podtrzymuj)
- Pozwalaj usuwać dodane sieci Wi-Fi
- Pozwalaj na konfiguracje prywatnego DNS

4 Zezwól na opcje programistyczne

- Jeśli zaznaczone, hasło serwisowe tymczasowo włączy opcje programistyczne na urządzeniu

5 Pozwalaj na dezaktywację

- Jeśli zaznaczone, hasło serwisowe pozwoli użytkownikowi na dezaktywację aplikacji Proget MDM na urządzeniu

6 Pozwalaj na przywrócenie do ustawień fabrycznych

- Jeśli zaznaczone, hasło serwisowe pozwoli użytkownikowi na przywrócenie urządzenia do ustawień fabrycznych

7 Awaryjny reset bazy danych

- Jeśli zaznaczone, hasło serwisowe autoryzuje awaryjny reset bazy danych aplikacji Proget MDM na urządzeniu
 - Użyj hasła serwisowego w aplikacji Proget w przypadku błędu synchronizacji aplikacji
- Nie można łączyć z innymi akcjami

8 Ustaw hasło

- Jeśli zaznaczone, hasło serwisowe pozwoli na ustawienie nowego hasła urządzenia w scenariuszu Direct Boot (po restarcie urządzenia)
 - Użyj hasła serwisowego, jeśli zapomnisz PIN-u do urządzenia. W tym celu zrestartuj urządzenie, kliknij w notyfikację Proget, wpisz wygenerowane hasło serwisowe i ustaw nowe

hasło na urządzeniu. Hasło serwisowe jest zależne od ustawień polityki 'Powiadomienia na zablokowanym ekranie'.

- Nie można łączyć z innymi akcjami

9 Data wygaśnięcia hasła serwisowego (na urządzeniu)

- Ustaw datę i godzinę, kiedy hasło serwisowe wygaśnie na urządzeniu
- Domyślna ważność to 24 godziny, minimalnie 5 minut, maksymalnie 30 dni

10 Generuj kod QR

- Jeśli zaznaczone, wraz z hasłem serwisowym zostanie wygenerowany kod QR do łatwiejszego zeskanowania na urządzeniu

11 Wyślij hasło serwisowe wiadomością email

- Jeśli zaznaczone, wygenerowane hasło serwisowe zostanie wysłane na podany adres email

12 Email

- Wprowadź adres email, na który zostanie wysłane hasło serwisowe
- Wymagane, jeśli zaznaczono 'Wyślij hasło serwisowe wiadomością email'

13 Język wiadomości

- Wybierz język, w którym zostanie wysłana wiadomość email z hasłem serwisowym

14 Generuj

14.1 Wygenerowane hasło serwisowe dla urządzenia

- Wyświetla wygenerowane hasło serwisowe dla urządzenia
- Hasło można skopiować do schowka za pomocą ikony kopiowania

14.2 Kod QR

- Wyświetla kod QR zawierający hasło serwisowe do zeskanowania na urządzeniu
- Widoczny tylko jeśli zaznaczono 'Generuj kod QR'

Android Enterprise Profile Owner (COPE)

Zaktualizowano: 16 lip 2026

Android Enterprise Profile Owner to typ aktywacji, w którym wszystkie działania są wykonywane w obszarze przestrzeni usług urządzenia. Ta aktywacja umożliwia podstawowe zarządzanie przestrzenią roboczą urządzeń.

Aktywacja Android Enterprise Profile Owner (COPE) umożliwia korzystanie z rozszerzonych funkcji ograniczających i konfigurujących urządzenia. Może być aktywowana tylko na urządzeniach z Androidem 11 lub wyższym, które zostały zresetowane do ustawień fabrycznych.

SAMSUNG SM-A225F

User:

Example User

Activation type:

Android Enterprise Profile Owner (COPE)

Alias:

Enter device alias

Last contact:

2026-05-22 11:48:37

Battery level: 69%

Health: Good

Internal storage: 5.2%

Total: 49.59 GiB (53.25 GB) Free: 47.01 GiB (50.48 GB)

RAM: 56.03%

Total: 3.63 GiB (3.89 GB) Free: 1.60 GiB (1.71 GB)

Generate service password

Details

Policy

Profiles

Applications

Location

Backups

Audit logs

Tasks

Dependency graph

File Manager

Reports

User accounts

Technical data

Manufacturer:

SAMSUNG

Model:

SM-A225F

OS:

Android 13 (33)

Serial number:

808F7XMPCHGA

IMEI 1:

3591467626779677

IMEI 2:

3591467626779679

Proget ID:

855 104

Activation date:

2026-05-22 11:44:17

App version:

2.20.1 (1201)

Patch version:

TP1A.220624.014.A225FXXSBDYE1

Bootloader version:

A225FXXSBDYE1

Security patch:

2025-05-01

System update status:

No info

CPU:

Mediatek MT6769V/CT (arm64-v8a)

Connection type:

Wi-Fi

IP:

192.168.3.142

Wi-Fi SSID:

<unknown ssid>

Roaming:

✗

Data encryption:

✓

Access to device usage data:

✓

Android Enterprise status:

Registered

Google Play services:

✓

Remote password change on the device:

✓

Access to background activity:

✓

Access to Wi-Fi management:

✓

Runtime permissions:

✓ Telephone ✗ SMS ✓ Call log ...

Groups

Example Group

Security

✗ 0

⚠ 0

✓ 2

ℹ 0

Root status 2026-05-22 11:44:18

Play Integrity verification status 2026-05-22 11:44:25

1

Informacje ogólne

1.1 Wprowadź alias urządzenia

- Ta akcja pozwala ustawić alias urządzenia. Alias może pomóc w identyfikacji urządzenia

1.2 Odśwież urządzenie

- Ta akcja pozwala wysłać polecenie odświeżenia do urządzenia w celu aktualizacji informacji i stanu urządzenia

1.3 Generuj hasło serwisowe

- Ta akcja pozwala wygenerować hasło serwisowe dla urządzenia, na którym nałożono tryb Utracony

2 Szybkie akcje

2.1 Pulpit zdalny

- Aby użyć tej akcji, na twoim urządzeniu musi być zainstalowana aplikacja Proget Remote. Proget Remote to aplikacja, która umożliwia zdalny dostęp do ekranu twojego urządzenia z serwera Proget

2.2 Zmień hasło służbowe

- Ta akcja pozwala wysłać polecenie do urządzenia, aby ustawić nowe hasło na kontenerze

2.3 Wyczyść dane urządzenia

- Ta akcja pozwala przywrócić ustawienia fabryczne

2.4 Wyczyść dane służbowe

- Ta akcja pozwala na usunięcie danych służbowych. Po wykonaniu tej akcji urządzenie zarejestrowane w konsoli Proget zostanie usunięte i dalsze zarządzanie tym urządzeniem nie będzie możliwe. Aplikacje Proget będą widoczne i kolejna rejestracja w konsoli Proget będzie możliwa

2.5 Zablokuj ekran urządzenia

- Ta akcja pozwala wysłać polecenie do urządzenia, które spowoduje zablokowanie ekranu urządzenia

2.6 Wyślij wiadomość

- Ta akcja pozwala na wysyłanie wiadomości. Podczas wykonywania tej akcji administrator może wybrać, jak wiadomość będzie widoczna na urządzeniu

2.7 Wiadomość alarmowa

- Ta akcja pozwala wysłać wiadomość alarmową. Podczas wykonywania tej akcji administrator musi ustawić treść wiadomości i może wybrać dodatkowe opcje. Wiadomość alertowa zostanie natychmiast wyświetlona na telefonie z charakterystycznym dźwiękiem i użytkownik będzie zmuszony potwierdzić, że przeczytał wiadomość

2.8 Przekieruj połączenia

- Ta akcja pozwala wysłać polecenie przekierowania połączeń telefonicznych na podany numer telefonu

2.9 Usuń przekierowanie połączeń

- Ta akcja pozwala wysłać polecenie usunięcia numeru, na który były przekierowane połączenia

2.10 Odśwież urządzenie

- Ta akcja pozwala wysłać polecenie odświeżenia do urządzenia w celu aktualizacji informacji i stanu urządzenia

2.11 Wymuś zmianę hasła urządzenia

- Ta akcja pozwala wysłać polecenie do urządzenia, które wymusi reset hasła

2.12 Wymuś zmianę hasła służbowego

- Ta akcja pozwala wysłać polecenie do urządzenia, które wymusi zmianę hasła

2.13 Reset blokady kontenera

- Ta akcja pozwala na zresetowanie blokady kontenera. Po wykonaniu tej akcji użytkownik będzie zmuszony ponownie wprowadzić hasło w przestrzeni roboczej.

2.14 Zablokuj kontener

- Ta akcja pozwala wysłać polecenie do urządzenia, które zablokuje przestrzeń roboczą

2.15 Odblokuj kontener

- Ta akcja pozwala wysłać polecenie do urządzenia, które odblokuje przestrzeń roboczą

2.16 Zweryfikuj urządzenie

- Ta akcja pozwala na weryfikację zgodności urządzenia z polityką Play Integrity

2.17 Wygeneruj dziennik zdarzeń

- Ta akcja pozwala wygenerować i wysłać logi audytowe na serwer Proget

3 Tabele

3.1 Podstawowe

3.2 Polityka

3.3 Profile

3.4 Aplikacje

3.5 Lokalizacja

3.6 Kopie zapasowe

3.7 Logi audytowe

3.8 Zadania

3.9 Graf zależności

3.10 File Manager

3.11 Raporty

Hasło serwisowe

Zaktualizowano: 9 cze 2026

NOWOŚĆ

Panel Hasło serwisowe umożliwia administratorowi wygenerowanie awaryjnego hasła serwisowego dla urządzenia. Hasło jest powiązane z konkretnym urządzeniem i ma określony czas ważności (domyślnie 24 godziny, minimalnie 5 minut, maksymalnie 30 dni). Działa nawet gdy urządzenie nie ma połączenia z internetem lub lokalna baza danych jest uszkodzona. Na aktywacji COPE akcja 'Odblokuj urządzenie' odblokowuje przestrzeń służbową (nie całe urządzenie), a profil Kiosk nie jest dostępny. Opcja 'Ustaw hasło' działa inaczej niż na Device Owner - kod jest generowany niezależnie (bez QR), można wybrać tylko datę ważności (bez godziny), a kod działa przez cały wybrany dzień (max 1 użycie dziennie). Po użyciu hasła serwisowego urządzenie wchodzi w 60-minutowe okno uprzywilejowanego działania, po czym wraca do stanu wymaganego przez polityki. Hasło można wpisać ręcznie lub zeskanować jako kod QR na urządzeniu.

Service password

* Select actions: ⓘ

- ☐ Unblock device
- ☐ Disable Kiosk
- ☐ Remove network restrictions ⓘ
- ☐ Allow developer options
- ☐ Allow deactivation
- ☐ Allow factory reset
- ☐ Emergency Database Reset ⓘ
- ☐ Set Password (COPE only) ⓘ

* Service password expiration date (on device):

2026-05-07 11:05



Time to expire: in about 24 hours

- ☒ Generate QR code
- ☒ Send service password via email

* Email:

example@domain.com

Message language:

English



Cancel

Generate

1 Odblokuj urządzenie

- Jeśli zaznaczone, hasło serwisowe odblokuje urządzenie z trybu Lost Mode

2 Wyłącz Kiosk

- Jeśli zaznaczone, hasło serwisowe wyjdzie z trybu Kiosk na urządzeniu

3 Usuń ograniczenia sieciowe

- Jeśli zaznaczone, hasło serwisowe tymczasowo usunie ograniczenia sieciowe na urządzeniu
 - Akcja ściąga restrykcje nałożone przez polityki związane z siecią:
 - Pozwalaj na zmianę ustawień sieci komórkowej
 - Pozwalaj używać danych komórkowych podczas roamingu

- Pozwalaj na konfigurację tetheringu oraz mobilnego punktu dostępu
- Pozwalaj edytować konfiguracje Wi-Fi
- Określ ustawienia konfiguracji podtrzymania Wi-Fi po uśpieniu (Zawsze podtrzymuj)
- Pozwalaj usuwać dodane sieci Wi-Fi
- Pozwalaj na konfiguracje prywatnego DNS (tylko COPE)

4 Zezwól na opcje programistyczne

- Jeśli zaznaczone, hasło serwisowe tymczasowo włączy opcje programistyczne na urządzeniu

5 Pozwalaj na dezaktywację

- Jeśli zaznaczone, hasło serwisowe pozwoli użytkownikowi na dezaktywację aplikacji Proget MDM na urządzeniu

6 Pozwalaj na przywrócenie do ustawień fabrycznych

- Jeśli zaznaczone, hasło serwisowe pozwoli użytkownikowi na przywrócenie urządzenia do ustawień fabrycznych

7 Awaryjny reset bazy danych

- Jeśli zaznaczone, hasło serwisowe autoryzuje awaryjny reset bazy danych aplikacji Proget MDM na urządzeniu
 - Użyj hasła serwisowego w aplikacji Proget w przypadku błędu synchronizacji aplikacji
- Nie można łączyć z innymi akcjami

8 Ustaw hasło (tylko COPE)

- Jeśli zaznaczone, hasło serwisowe pozwoli na ustawienie nowego hasła przestrzeni służbowej urządzenia w scenariuszu Direct Boot (po restarcie urządzenia)
 - Użyj hasła serwisowego, jeśli zapomnisz PIN-u do urządzenia. W tym celu zrestartuj urządzenie, kliknij w notyfikację Proget i wpisz wygenerowane hasło serwisowe
- Nie można łączyć z innymi akcjami

9 Data wygaśnięcia hasła serwisowego (na urządzeniu)

- Ustaw datę i godzinę, kiedy hasło serwisowe wygaśnie na urządzeniu
- Domyślna ważność to 24 godziny, minimalnie 5 minut, maksymalnie 30 dni

10 Generuj kod QR

- Jeśli zaznaczone, wraz z hasłem serwisowym zostanie wygenerowany kod QR do łatwiejszego zeskanowania na urządzeniu

11 Wyślij hasło serwisowe wiadomością email

- Jeśli zaznaczone, wygenerowane hasło serwisowe zostanie wysłane na podany adres email

12 Email

- Wprowadź adres email, na który zostanie wysłane hasło serwisowe
- Wymagane, jeśli zaznaczono 'Wyślij hasło serwisowe wiadomością email'

13 Język wiadomości

- Wybierz język, w którym zostanie wysłana wiadomość email z hasłem serwisowym

14 Generuj

14.1 Wygenerowane hasło serwisowe dla urządzenia

- Wyświetla wygenerowane hasło serwisowe dla urządzenia
- Hasło można skopiować do schowka za pomocą ikony kopiowania

14.2 Kod QR

- Wyświetla kod QR zawierający hasło serwisowe do zeskanowania na urządzeniu
- Widoczny tylko jeśli zaznaczono 'Generuj kod QR'

Android

Zaktualizowano: 16 lip 2026

Android to najprostszy typ aktywacji, który pozwala zarządzać przestrzenią urządzenia z poziomu konsoli Proget. Posiada podstawowe funkcjonalności systemu, umożliwiające zdalne zarządzanie urządzeniami mobilnymi.

GOOGLE Pixel XL

User:
Example User

Activation type:
Android

Alias:
Enter device alias

Last contact:
2026-05-13 13:17:43

Battery level: 100%

Health: Good

Internal storage: 24.06%

Total: 24.32 GiB (26.11 GB) Free: 18.47 GiB (19.83 GB)

External storage:
No external memory card

RAM: 50.78%

Total: 3.68 GiB (3.95 GB) Free: 1.81 GiB (1.94 GB)

Generate service password

Details

Policy

Profiles

Applications

Location

Backups

Audit logs

Tasks

Dependency graph

Reports

Export

User accounts

Technical data

Manufacturer:GOOGLE

Model:Pixel XL

OS:Android 10 (29)

Serial number:No info

IMEI :UNDEFINED

Proget ID:988 801

Activation date:2026-05-13 07:30:09

App version:2.20 (1200)

Patch version:QP1A.191005.007.A3

Bootloader version:8996-012001-1908071822

Security patch:2019-10-06

System update status:No info

CPU:null null (arm64-v8a)

Connection type:Wi-Fi

IP:192.168.2.217

Wi-Fi MAC:8c:30:88:42:a3:96

Wi-Fi SSID:ProgetUnifi

Roaming:✗

Data encryption:✓

Access to device usage data:✓

Android Enterprise status:Not applicable

Google Play services:✓

Access to background activity:✓

Access to Wi-Fi management:✓

Runtime permissions:✓ Telephone ✓ SMS ✓ Call log ...

Groups

Example Group

Security

No password on the device

2026-05-13 07:30:14

The lack of a password on the device allows access to the data by unauthorized persons.

1

Informacje ogólne

1.1 Wprowadź alias urządzenia

- Ta akcja pozwala ustawić alias urządzenia. Alias może pomóc w identyfikowaniu urządzenia

1.2 Odśwież urządzenie

- Ta akcja pozwala wysłać polecenie odświeżenia do urządzenia w celu aktualizacji informacji oraz statusu urządzenia

1.3 Generuj hasło serwisowe

- Ta akcja pozwala na wygenerowanie hasła serwisowego dla urządzenia, na którym nałożono Lost Mode

2 Szybkie akcje

2.1 Zdalny pulpit

- Aby użyć tej akcji, na urządzeniu musi być zainstalowana aplikacja Proget Remote. Proget Remote to aplikacja umożliwiająca zdalny dostęp do ekranu urządzenia Android z serwera Proget

2.2 Resetuj hasło

- Ta akcja pozwala wysłać polecenie do urządzenia, które wywoła prośbę o zresetowanie hasła

2.3 Zmień hasło

- Ta akcja pozwala wysłać polecenie do urządzenia w celu ustawienia nowego hasła

2.4 Wyczyść dane urządzenia

- Ta akcja pozwala przywrócić ustawienia fabryczne

2.5 Wyczyść dane służbowe

- Ta akcja pozwala na wymazanie danych firmy. Po wykonaniu tej akcji urządzenie zarejestrowane w konsoli Proget zostanie usunięte i dalsze zarządzanie tym urządzeniem nie będzie możliwe. Aplikacje Proget będą widoczne i możliwa będzie kolejna rejestracja w konsoli Proget

2.6 Zablokuj ekran urządzenia

- Ta akcja pozwala wysłać polecenie do urządzenia, które wywoła blokadę ekranu urządzenia

2.7 Wyślij wiadomość

- Ta akcja pozwala wysłać wiadomość. Podczas wykonywania tej akcji administrator może wybrać, jak wiadomość będzie widoczna na urządzeniu

2.8 Wiadomość alarmowa

- Ta akcja pozwala wysłać wiadomość alarmową. Podczas wykonywania tej akcji administrator musi ustawić treść wiadomości i może wybrać dodatkowe opcje. Wiadomość alarmowa będzie natychmiast widoczna na telefonie z charakterystycznym dźwiękiem i użytkownik będzie zmuszony potwierdzić, że przeczytał wiadomość

2.9 Przekieruj połączenia

- Ta akcja pozwala wysłać polecenie przekierowania połączeń telefonicznych na podany numer telefonu

2.10 Usuń przekierowanie połączeń

- Ta akcja pozwala wysłać polecenie usunięcia numeru, na który były przekierowane połączenia

2.11 Odśwież urządzenie

- Ta akcja pozwala wysłać polecenie odświeżenia do urządzenia w celu aktualizacji informacji oraz statusu urządzenia

2.12 Zweryfikuj urządzenie

- Ta akcja pozwala na weryfikację zgodności urządzenia z polityką Play Integrity

2.13 Wygeneruj dziennik zdarzeń

- Ta akcja pozwala wygenerować i wysłać logi audytowe na serwer Proget
-

3.1 Podstawowe

3.2 Polityka

3.3 Profile

3.4 Aplikacje

3.5 Lokalizacja

3.6 Kopie zapasowe

3.7 Logi audytowe

3.8 Zadania

3.9 Graf zależności

3.10 Raporty

3.11 Eksport

Hasło serwisowe

Zaktualizowano: 9 cze 2026

NOWOŚĆ

Panel Hasło serwisowe umożliwia administratorowi wygenerowanie awaryjnego hasła serwisowego dla urządzenia. Hasło jest powiązane z konkretnym urządzeniem i ma określony czas ważności (domyślnie 24 godziny, minimalnie 5 minut, maksymalnie 30 dni). Działa nawet gdy urządzenie jest w trybie Lost Mode, nie ma połączenia z internetem lub lokalna baza danych jest uszkodzona. Po użyciu urządzenie wchodzi w 60-minutowe okno uprzywilejowanego działania, po czym wraca do stanu wymaganego przez polityki. Hasło można wpisać ręcznie lub zeskanować jako kod QR na urządzeniu.



Service password

* Select actions: ⓘ

- ☐ Unblock device
- ☐ Disable Kiosk
- ☐ Remove network restrictions ⓘ
- ☐ Allow developer options
- ☐ Allow deactivation
- ☐ Allow factory reset
- ☐ Emergency Database Reset ⓘ
- ☐ Set Password ⓘ

* Service password expiration date (on device):

2026-05-07 11:19



Time to expire: in 1 day

- ☒ Generate QR code
- ☒ Send service password via email

* Email:

example@domain.com

Message language:

English



Cancel

Generate

1 Odblokuj urządzenie

- Jeśli zaznaczone, hasło serwisowe odblokuje urządzenie z trybu Lost Mode

2 Wyłącz Kiosk

- Jeśli zaznaczone, hasło serwisowe wyjdzie z trybu Kiosk na urządzeniu

3 Usuń ograniczenia sieciowe

- Jeśli zaznaczone, hasło serwisowe tymczasowo usunie ograniczenia sieciowe na urządzeniu
 - Akcja ściąga restrykcje nałożone przez polityki związane z siecią:
 - Pozwalaj na zmianę ustawień sieci komórkowej
 - Pozwalaj używać danych komórkowych podczas roamingu

- Pozwalaj na konfigurację tetheringu oraz mobilnego punktu dostępu
- Pozwalaj edytować konfiguracje Wi-Fi
- Określ ustawienia konfiguracji podtrzymania Wi-Fi po uśpieniu (Zawsze podtrzymuj)
- Pozwalaj usuwać dodane sieci Wi-Fi
- Pozwalaj na konfiguracje prywatnego DNS

4 Zezwól na opcje programistyczne

- Jeśli zaznaczone, hasło serwisowe tymczasowo włączy opcje programistyczne na urządzeniu

5 Pozwalaj na dezaktywację

- Jeśli zaznaczone, hasło serwisowe pozwoli użytkownikowi na dezaktywację aplikacji Proget MDM na urządzeniu

6 Pozwalaj na przywrócenie do ustawień fabrycznych

- Jeśli zaznaczone, hasło serwisowe pozwoli użytkownikowi na przywrócenie urządzenia do ustawień fabrycznych

7 Awaryjny reset bazy danych

- Jeśli zaznaczone, hasło serwisowe autoryzuje awaryjny reset bazy danych aplikacji Proget MDM na urządzeniu
 - Użyj hasła serwisowego w aplikacji Proget w przypadku błędu synchronizacji aplikacji
- Nie można łączyć z innymi akcjami

8 Ustaw hasło

- Jeśli zaznaczone, hasło serwisowe pozwoli na ustawienie nowego hasła urządzenia w scenariuszu Direct Boot (po restarcie urządzenia)
 - Użyj hasła serwisowego, jeśli zapomnisz PIN-u do urządzenia. W tym celu zrestartuj urządzenie, kliknij w notyfikację Proget, wpisz wygenerowane hasło serwisowe i ustaw nowe hasło na urządzeniu. Hasło serwisowe jest zależne od ustawień polityki 'Powiadomienia na zablokowanym ekranie'.

- Nie można łączyć z innymi akcjami

9 Data wygaśnięcia hasła serwisowego (na urządzeniu)

- Ustaw datę i godzinę, kiedy hasło serwisowe wygaśnie na urządzeniu
- Domyślna ważność to 24 godziny, minimalnie 5 minut, maksymalnie 30 dni

10 Generuj kod QR

- Jeśli zaznaczone, wraz z hasłem serwisowym zostanie wygenerowany kod QR do łatwiejszego zeskanowania na urządzeniu

11 Wyślij hasło serwisowe wiadomością email

- Jeśli zaznaczone, wygenerowane hasło serwisowe zostanie wysłane na podany adres email

12 Email

- Wprowadź adres email, na który zostanie wysłane hasło serwisowe
- Wymagane, jeśli zaznaczono 'Wyślij hasło serwisowe wiadomością email'

13 Język wiadomości

- Wybierz język, w którym zostanie wysłana wiadomość email z hasłem serwisowym

14 Generuj

14.1 Wygenerowane hasło serwisowe dla urządzenia

- Wyświetla wygenerowane hasło serwisowe dla urządzenia
- Hasło można skopiować do schowka za pomocą ikony kopiowania

14.2 Kod QR

- Wyświetla kod QR zawierający hasło serwisowe do zeskanowania na urządzeniu
- Widoczny tylko jeśli zaznaczono 'Generuj kod QR'

iOS (Tryb nadzorowany)

Zaktualizowano: 16 lip 2026

Aktywacja nadzorowana urządzenia iOS umożliwia korzystanie z rozszerzonych funkcji ograniczających i konfigurujących urządzenie. Aby z niej skorzystać, potrzebna jest odpowiednia konfiguracja Apple Business Manager oraz urządzenie z systemem operacyjnym iOS.

APPLE iPhone17,3

User:

Example User

Activation type:

iOS (Supervised mode)

Alias:

Enter device alias

Last contact:

2026-05-22 10:24:06

Battery level: 100%

Internal storage: 15.32%

Total: 128.00 GiB (137.44 GB) Free: 108.39 GiB (116.39 GB)

External storage:

No external memory card

Details

Policy

Profiles

Applications

Location

Audit logs

Tasks

Dependency graph

File Manager

Technical data

Manufacturer:	APPLE
Model:	iPhone17,3
OS:	iOS 26.4.2
Serial number:	XXXXXXXXXXXX
IMEI 1:	XXXXXXXXXXXX
IMEI 2:	XXXXXXXXXXXX
Proget ID:	867 367
Activation date:	2026-05-22 10:23:46
System update status:	Update available
Declarative management:	✓
Update Version:	26.5
Wi-Fi MAC:	XXXXXXXXXXXX
Roaming:	✗
Data encryption:	✓
Lost mode enabled:	✗

Groups

Example Group

Security

✗ 0

⚠ 0

✓ 1

ℹ 0

Device secured

1.1 Wprowadź alias urządzenia

- Ta akcja umożliwia ustawienie aliasu urządzenia. Alias może pomóc w identyfikacji urządzenia

1.2 Odśwież urządzenie

- Ta akcja pozwala na wysłanie polecenia odświeżenia do urządzenia w celu aktualizacji informacji i statusu urządzenia

2 Szybkie akcje

2.1 Resetuj hasło

- Ta akcja pozwala na wysłanie do urządzenia polecenia, które spowoduje żądanie zresetowania hasła

2.2 Wyczyść dane urządzenia

- Ta akcja pozwala na przywrócenie ustawień fabrycznych urządzenia

2.3 Wyczyść dane służbowe

- Ta akcja pozwala na usunięcie danych firmowych. Po wykonaniu tej akcji urządzenie zarejestrowane w konsoli Proget zostanie usunięte, a dalsze zarządzanie tym urządzeniem nie będzie możliwe. Aplikacje Proget będą widoczne, a kolejna rejestracja w konsoli Proget będzie możliwa

2.4 Zablokuj ekran urządzenia

- Ta akcja pozwala na wysłanie do urządzenia polecenia, które zablokuje ekran urządzenia

2.5 Odśwież urządzenie

- Ta akcja pozwala na wysłanie polecenia odświeżenia do urządzenia w celu aktualizacji informacji i statusu urządzenia

2.6 Włącz tryb Utracony

- Ta akcja pozwala na wysłanie polecenia zablokowania urządzenia. Gdy urządzenie jest zablokowane, użytkownik może zadzwonić tylko do administratora lub na wcześniej wprowadzony numer alarmowy

2.7 Wyłącz tryb Utracony

- Ta akcja pozwala na wysłanie polecenia odblokowania urządzenia

2.8 Wyślij Custom Apple Command

- Ta akcja pozwala na wysłanie Custom Apple Command do urządzenia

3 Tabele

3.1 Podstawowe

3.2 Polityka

3.3 Profile

3.4 Aplikacje

3.5 Lokalizacja

3.6 Logi audytowe

3.7 Zadania

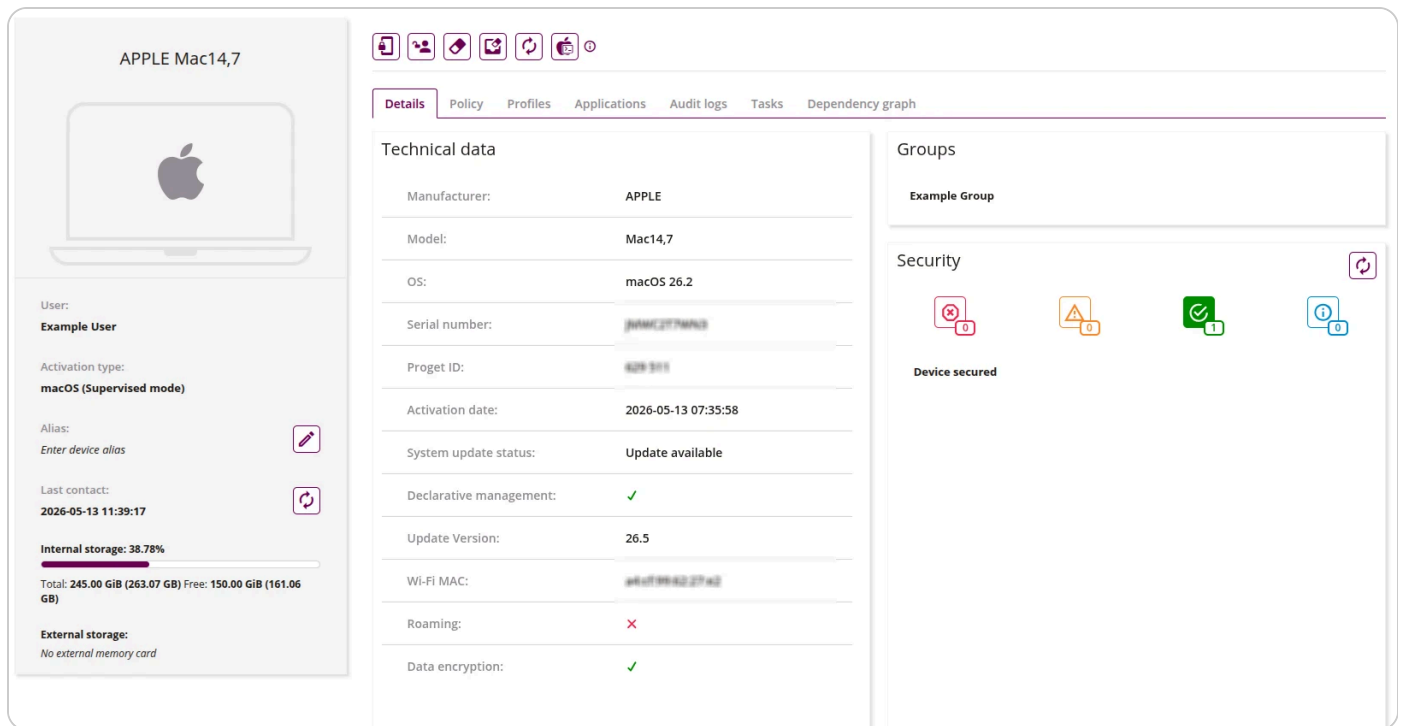
3.8 Graf zależności

3.9 File Manager

macOS

Zaktualizowano: 16 lip 2026

Aktywacja urządzenia macOS umożliwia korzystanie z funkcji ograniczających i konfigurujących urządzenie. Możesz to wykonać na urządzeniu z systemem operacyjnym macOS.



1 Informacje ogólne

1.1 Wprowadź alias urządzenia

- Ta akcja pozwala ustawić alias urządzenia. Alias może pomóc w identyfikacji urządzenia

1.2 Odśwież urządzenie

- Ta akcja pozwala na wysłanie polecenia odświeżenia do urządzenia w celu aktualizacji informacji i statusu urządzenia

2 Szybkie akcje

2.1 Zablokuj urządzenie

- Ta akcja pozwala na wysłanie polecenia blokady urządzenia

2.2 Odblokuj urządzenie

- Ta akcja pozwala na wysłanie polecenia odblokowania urządzenia

2.3 Wyczyść dane urządzenia

- Ta akcja pozwala na przywrócenie ustawień fabrycznych

2.4 Wyczyść dane służbowe

- Ta akcja pozwala na usunięcie danych służbowych. Po wykonaniu tej akcji urządzenie zarejestrowane w konsoli Proget zostanie usunięte, a dalsze zarządzanie tym urządzeniem nie będzie możliwe. Aplikacje Proget będą widoczne, a kolejna rejestracja w konsoli Proget będzie możliwa

2.5 Odśwież urządzenie

- Ta akcja pozwala na wysłanie polecenia odświeżenia do urządzenia w celu aktualizacji informacji i statusu urządzenia

2.6 Wyślij Custom Apple Command

- Ta akcja pozwala na wysłanie Custom Apple Command do urządzenia
-

3 Tabele

3.1 Podstawowe

3.2 Polityka

3.3 Profile

3.4 Aplikacje

3.5 Logi audytowe

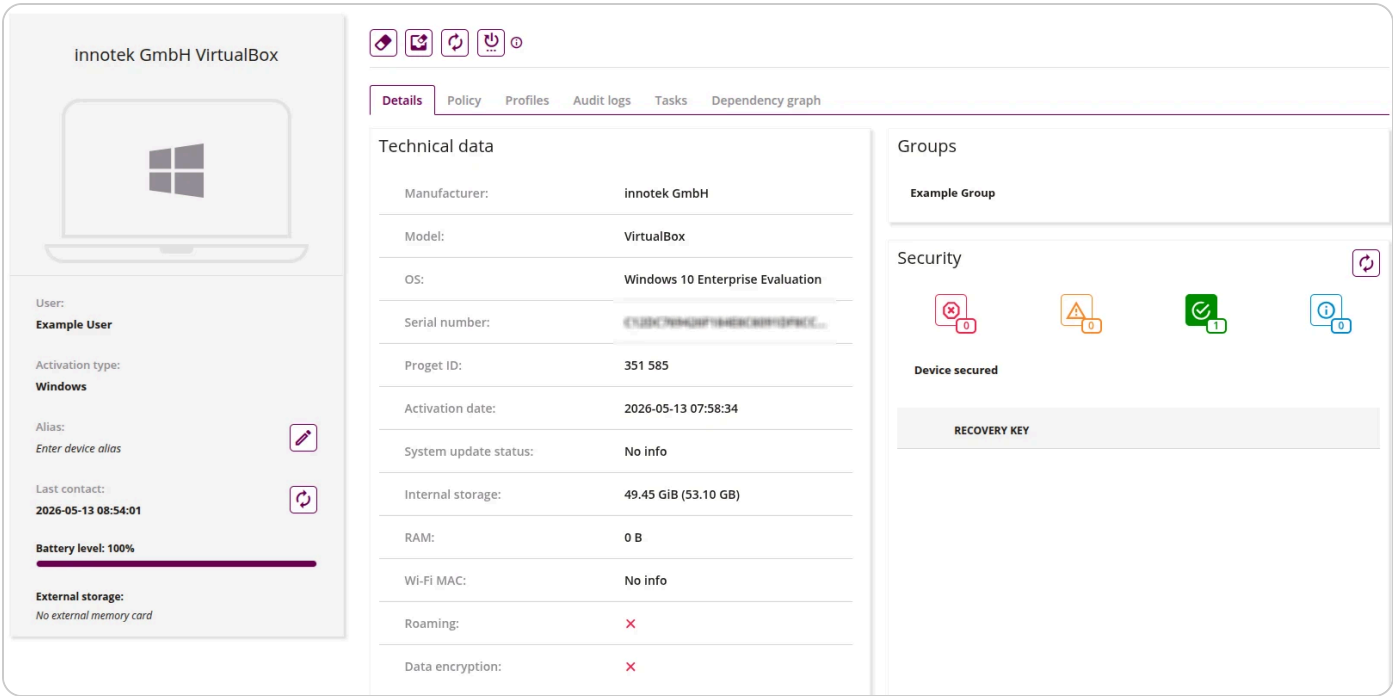
3.6 Zadania

3.7 Graf zależności

Windows

Zaktualizowano: 16 lip 2026

Aktywacja urządzenia Windows umożliwia korzystanie z funkcji ograniczających i konfigurujących urządzenie. Możesz to wykonać na urządzeniu z systemem operacyjnym Windows.



1 Informacje ogólne

1.1 Wprowadź alias urządzenia

- Ta akcja pozwala ustawić alias urządzenia. Alias może pomóc w identyfikacji urządzenia

1.2 Odśwież urządzenie

- Ta akcja pozwala na wysłanie polecenia odświeżenia do urządzenia w celu aktualizacji informacji i statusu urządzenia

2 Szybkie akcje

2.1 Wyczyść dane urządzenia

- Ta akcja pozwala na przywrócenie ustawień fabrycznych

2.2 Wyczyść dane służbowe

- Ta akcja pozwala na usunięcie danych służbowych. Po wykonaniu tej akcji urządzenie zarejestrowane w konsoli Proget zostanie usunięte, a dalsze zarządzanie tym urządzeniem nie będzie możliwe. Aplikacje Proget będą widoczne, a kolejna rejestracja w konsoli Proget będzie możliwa

2.3 Odśwież urządzenie

- Ta akcja pozwala na wysłanie polecenia odświeżenia do urządzenia w celu aktualizacji informacji i statusu urządzenia

2.4 Restartuj urządzenie

- Ta akcja pozwala na wysłanie polecenia do urządzenia w celu jego ponownego uruchomienia

3 Tabele

3.1 Podstawowe

3.2 Polityka

3.3 Profile

3.4 Logi audytowe

3.5 Zadania

3.6 Graf zależności

Zakładki urządzeń

Zaktualizowano: 16 lip 2026

Kliknij w interesującą Cię kartę urządzenia, aby uzyskać szczegółowe informacje.



Podstawowe

Szczegóły urządzenia, zastosowana polityka i stan zabezpieczeń



Polityka

Monitorowanie przypisanej polityki i weryfikacja zgodności



Profile

Profile przypisane do urządzenia z grup lub bezpośrednio



Aplikacje

Zainstalowane aplikacje wraz z dostępnymi akcjami



Lokalizacja

Wcześniejsze lokalizacje i wymuszenie lokalizacji urządzenia



Kopie zapasowe

Tworzenie i przegląd kopii zapasowych kontaktów, SMS-ów i połączeń



Logi audytowe

Generowanie i przegląd logów audytowych urządzenia



Zadania

Wszystkie zadania wygenerowane dla tego urządzenia



Graf zależności

Interaktywny graf powiązań urządzenia z innymi elementami



File Manager

Zdalne przeglądanie, wgrywanie i zarządzanie plikami urządzenia



Raporty

Tworzenie i przegląd raportów użycia urządzenia



Eksport

Eksport SMS-ów, kontaktów i listy połączeń z urządzenia



Konta użytkownika



Raporty o błędach systemowych

Lista wszystkich kont użytkownika
dodanych na urządzeniu

Generowanie raportów błędów
Android, usuwanych po 30 dniach



Zdjęcia z blokady

Zdjęcia wykonane podczas blokady
urządzenia



Użytkownicy

Użytkownicy, którzy zalogowali się do
kiosku, wraz z parametrami

Podstawowe

Zaktualizowano: 24 cze 2025

Tutaj znajdziesz szczegóły dotyczące urządzenia, zastosowanej polityki i bezpieczeństwa urządzenia. Możesz również przypisać polityki bezpośrednio do urządzenia.

Technical data		Groups	
Manufacturer:	SAMSUNG	Example Group	
Model:	SM-A225F		
OS:	Android 13 (33)		
Serial number:	XXXXXXXXXX		
IMEI 1:	XXXXXXXXXXXX		
IMEI 2:	354476280777073		
Proget ID:	698 357		
Activation date:	2025-10-17 09:26:47		
App version:	2.19.0 (1111)		
Patch version:	TP1A.220624.014.A225FXXSBDYE1		
Bootloader version:	A225FXXSBDYE1		
Security patch:	2025-05-01		
System update status:	No info		
CPU:	Mediatek MT6769V/CT (arm64-v8a)		
Connection type:	WiFi		
IP:	192.168.1.1		
Wi-Fi MAC:	XX:XX:XX:XX:XX:XX		
Wi-Fi SSID:	PROGET-1		
Roaming:	✗		
Data encryption:	✓		
Access to device usage data:	✓		
Android Enterprise status:	Registered		
Google Play services:	✓		
Remote password change on the device:	✓		
Lost mode enabled:	✗		
Access to background activity:	✓		
Access to Wi-Fi management:	✓		
Runtime permissions:	✓ Telephone ✓ SMS ✓ Call log ✓ ...		
		Security	
		✗0 ⚠0 ✓2 i0	
		Root status	
		2025-10-17 09:26:48	
		Play Integrity verification status	
		2025-10-17 09:26:57	

- Tutaj możesz zobaczyć najważniejsze dane techniczne swojego urządzenia, takie jak:
 - Producent urządzenia
 - Model urządzenia
 - IMEI urządzenia
 - Wi-Fi SSID
 - Wersja aplikacji Proget, itp

2 Grupy

- Tutaj możesz zobaczyć grupy, które są obecnie przypisane do urządzenia

3 Bezpieczeństwo

- Tutaj możesz zobaczyć status bezpieczeństwa swojego urządzenia. W systemie Proget są cztery typy statusu bezpieczeństwa, takie jak:
 - Bezpieczne
 - Niebezpieczne
 - Informacyjne
 - Krytyczne
- Przykłady statusów, które można tutaj znaleźć:
 - Brak hasła na urządzeniu
 - Status root
 - Status weryfikacji Play Integrity

Polityka

Zaktualizowano: 12 lut 2025

W tym miejscu możesz monitorować politykę nadaną przez administratora i sprawdzić, czy została poprawnie zastosowana na urządzeniu. Możesz także porównać oczekiwane ustawienia z rzeczywistą konfiguracją w celu zweryfikowania zgodności.

Device policy

Default policy (Allocation: Default)

Matching: 68

Modification date: 2025-07-08 14:31:52

Management

1 Polityka urządzenia

- Informacja o nazwie i przydziale przypisanej polityki do urządzenia
- Po kliknięciu na nazwę polityki użytkownik zostanie przekierowany do jej konfiguracji

2 Dopasowanie

2.1 Filtr polityki

- Wyszukuj polityki filtrując po:
 - Status
 - Dopasowane
 - Niedopasowane
 - Nazwa
 - Zaczynij wpisywać nazwę polityki, a wyniki będą filtrowane dynamicznie
 - Kategoria
 - Aplikacje
 - Funkcjonalność
 - Lokalizacja
 - Hasło
 - Bezpieczeństwo

2.2 Tabela dopasowania polityki

- Informacje o politykach dostępne w tabeli:
 - Dopasowanie polityk
 - Kategoria polityk
 - Aktualny stan polityk na urządzeniu
 - Wymagany stan polityk na urządzeniu
 - Szczegóły polityk

3 Zarządzenie

3.1 Edytuj politykę na urządzeniu

- Akcja ta pozwala na edycję polityki bezpośrednio przypisanej do urządzenia

3.2 Nałóż ponownie politykę

- Akcja ta pozwala na ponowne wysłanie polityki do urządzenia

Profile

Zaktualizowano: 3 gru 2024

Tutaj znajdziesz wszystkie profile przypisane do tego urządzenia, profile przypisane z grupy oraz profile przypisane bezpośrednio. Stąd możesz przypisać profile bezpośrednio do urządzenia.

Device profiles

Selected: 0

Deselect all



Edit



☐	PROFILE NAME	CATEGORY	ALLOCATION
☐	Example Business Documents profile	Business documents	ExampleGroup
☐	Example Kiosk profile	Kiosk	ExampleGroup
☐	Example location profile	Location	Device

Results: 3

Page limit:

50



1 Usun profil

- Ta akcja pozwala usunąć dodany profil

2 Edytuj

- Ta akcja pozwala edytować profile na urządzeniu. Możesz zarządzać profilami na swoim urządzeniu, dodając je i usuwając

3 Odśwież

- Ta akcja pozwala odświeżyć listę profili

4 Lista profili

- Lista wszystkich profili dodanych do urządzenia. Lista zawiera informacje, czy profile są dodane bezpośrednio do urządzenia czy z grupy

Aplikacje

Zaktualizowano: 24 cze 2025

Tutaj znajdziesz tabelę z informacjami o aplikacjach zainstalowanych na danym urządzeniu. Możesz dodawać aplikacje do urządzenia i wykonywać na nich akcje.

Applications

Matching: 5

Modification date: 2025-06-03 09:25:21

All applications

Management

1

Dopasowanie

1.1 Filtry

- Filtr aplikacji pozwala szukać aplikacji według danych, takich jak:
 - Status
 - Nazwa aplikacji
 - ID aplikacji

1.2 Synchronizuj aplikację

- Ta akcja pozwala na zsynchronizowanie statusu aplikacji na urządzeniu

1.3 Odśwież dane

- Ta akcja pozwala na odświeżenie danych aplikacji zarządzanych przez konsolę Proget

1.4 Lista aplikacji

- Lista wszystkich zarządzanych aplikacji wraz z ich statusem

2 Wszystkie aplikacje

2.1 Filtry

- Filtr aplikacji pozwala szukać aplikacji według danych, takich jak:
 - Nazwa aplikacji
 - ID aplikacji
 - Zainstalowane przez
 - Zablokowane

2.2 Wyczyść dane aplikacji

- Ta akcja pozwala na wyczyszczenie danych aplikacji na urządzeniu poprzez wysłanie akcji z konsoli

2.3 Wyłącz aplikację

- Ta akcja pozwala na wyłączenie aplikacji na urządzeniu poprzez wysłanie akcji z konsoli

2.4 Włącz aplikację

- Ta akcja pozwala na włączenie zablokowanej aplikacji na urządzeniu poprzez wysłanie akcji z konsoli

2.5 Uruchom aplikację

- Ta akcja pozwala na uruchomienie aplikacji na urządzeniu poprzez wysłanie akcji z konsoli

2.6 Usuń aplikację

- Ta akcja pozwala na usunięcie aplikacji z urządzenia poprzez wysłanie akcji z konsoli

2.7 Lista aplikacji

- Lista wszystkich aplikacji na urządzeniu wraz z ich parametrami

3 Zarządzanie

3.1 Wyczyść dane aplikacji

- Ta akcja pozwala na wyczyszczenie danych aplikacji na urządzeniu poprzez wysłanie akcji z konsoli

3.2 Uruchom aplikację

- Ta akcja pozwala na uruchomienie aplikacji na urządzeniu poprzez wysłanie akcji z konsoli

3.3 Wyślij konfigurację

- Ta akcja pozwala na wysłanie konfiguracji do aplikacji na urządzeniu poprzez wysłanie akcji z konsoli, np. dla aplikacji Gmail

3.4 Edytuj

- Ta akcja pozwala na edycję listy aplikacji i przygotowanie instalacji aplikacji służbowych na urządzeniu

3.5 Odśwież dane

- Ta akcja pozwala na odświeżenie listy aplikacji

3.6 Lista aplikacji

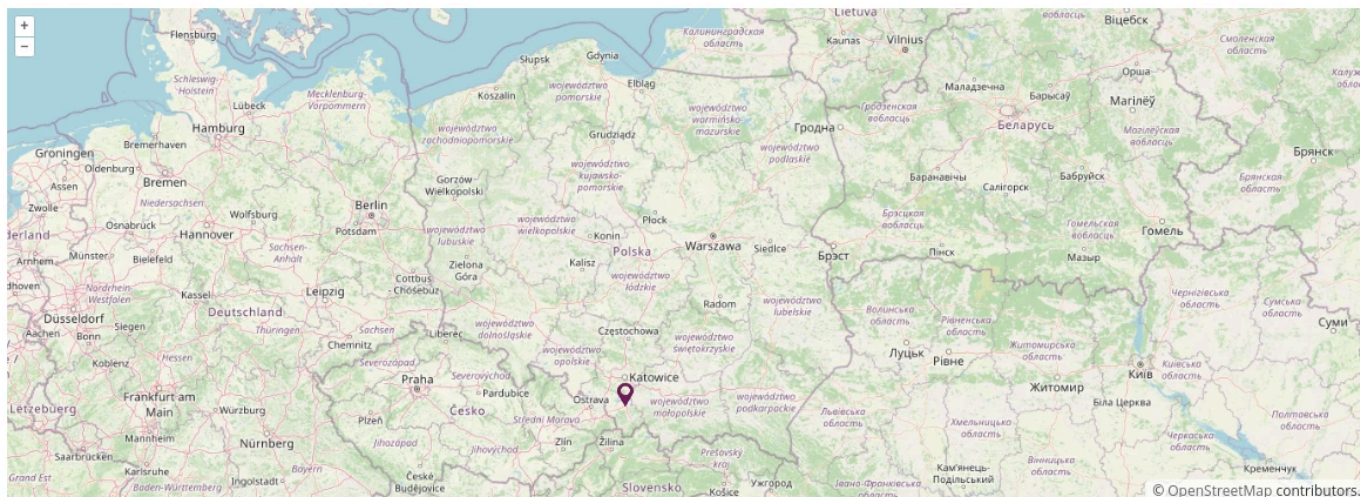
- Lista wszystkich zarządzanych aplikacji na urządzeniu

Lokalizacja

Zaktualizowano: 3 gru 2024

Tutaj możesz sprawdzić listę wcześniej pobranych lokalizacji tego urządzenia. Możesz również wymusić lokalizację urządzenia w tym momencie.

Location



Location History

Date: From Select ... To Select date

Reset filters

☐ Show route on the map

Force location



DATE	LATITUDE	LONGITUDE	ALTITUDE	SPEED	ACCURACY
2020-11-02 09:14:01	49.85227789	19.14062500	248.3	0 km/h	13.44
2020-11-02 09:14:08	49.85227789	19.14062500	248.3	0 km/h	13.44

Results: 2 | Page limit: 50



1 Mapa lokalizacji

- Na tej mapie możesz zobaczyć lokalizację urządzenia, która jest wskazana przez pinezki

2 Data

- Ta funkcjonalność pozwala sprawdzić lokalizację urządzenia w wybranych okresach czasu

3 Pokaż trasę na mapie

- Ta funkcjonalność pokazuje trasę od najstarszej lokalizacji do najnowszej, czyli trasę, którą przemieszczało się urządzenie

4**Wymuś lokalizację**

- Ta akcja pozwala wymusić aktualną lokalizację urządzenia

5**Odśwież**

- Ta akcja pozwala odświeżyć listę lokalizacji

6**Lista lokalizacji**

- Lista wszystkich lokalizacji urządzenia oraz ich parametrów

Kopie zapasowe

Zaktualizowano: 3 gru 2024

Tutaj możesz wykonać kopię zapasową oraz znaleźć wszystkie wcześniej wykonane kopie zapasowe z tego urządzenia. Dostępne opcje kopii zapasowej to kopia kontaktów, kopia SMS/MMS oraz kopia rejestru połączeń.

Backup of this device

Selected: 0 | Deselect all



Make a backup 

☐	DATE
☐	2024-10-02 12:39

Results: 1 | Page limit: 50 

Other backup

Selected: 0 | Deselect all





☐	DEVICE	ID	DATE
☐	Hammer Iron V	2024-10-02 12:47	2024-10-02 12:47

Results: 1 | Page limit: 10 

1 Przywróć

- Ta akcja pozwala na przywrócenie dostępnych kopii zapasowych na Twoim urządzeniu

2 Usuń

- Ta akcja pozwala na usunięcie dostępnych kopii zapasowych

3 Wykonaj kopię zapasową

- Ta akcja pozwala na stworzenie kopii zapasowej urządzenia, takiej jak:
 - Kopia kontaktów
 - Kopia SMS/MMS
 - Kopia rejestru połączeń

4 Odśwież

- Ta akcja pozwala na odświeżenie listy kopii zapasowych, jeśli wygenerowana kopia nie jest wyświetlana

5 Lista kopii zapasowych

- Lista wygenerowanych kopii zapasowych

6 Przywróć

- Ta akcja pozwala na przywrócenie dostępnych kopii zapasowych na innych urządzeniach

7 Usuń

- Ta akcja pozwala na usunięcie dostępnych kopii zapasowych

8 Odśwież

- Ta akcja pozwala na odświeżenie listy innych kopii zapasowych

9 Inna lista kopii zapasowych

- Lista wszystkich wykonanych kopii zapasowych wraz z ich parametrami

Logi audytowe

Zaktualizowano: 3 gru 2024

Tutaj możesz znaleźć wszystkie wygenerowane logi powiązane z urządzeniem.

Audit logs

Action: Select

Status: Select

Date of occurrence: From Select To Select

Reset filters

ACTION	STATUS	DATE OF OCCURRENCE	PERFORMED BY	PERFORMED ON	DETAILS
device.activate	Success	2024-10-02 12:41:45	SAMSUNG SM-A22...	SAMSUNG SM-A22...	Device activated
device.ownership....	Success	2024-10-02 12:41:44	SAMSUNG SM-A22...	SAMSUNG SM-A22...	Device ownership updated

Results: 2 | Page limit: 50

1

Filtr

- Użyj filtrów, aby wyszukać odpowiedni log

2

Wyszukiwarka

- Użyj wyszukiwarki, aby wyszukać odpowiedni log

3

Lista logów

- Lista logów, które zostały wygenerowane w wyniku określonej akcji w konsoli lub na urządzeniu

Zadania

Zaktualizowano: 3 gru 2024

Tutaj znajdziesz wszystkie zadania wygenerowane na tym urządzeniu.

Tasks

Complete date:



Action:



Created by:



Status:



[Reset filters](#)



SENT DATE	COMPLETE DATE	ACTION	CREATED BY	STATUS
2024-10-02 13:23:36	2024-10-02 13:23:53	Export calls	example	Success
2024-10-02 13:23:33	2024-10-02 13:23:53	Export contacts	example	Success
2024-10-02 13:23:31	2024-10-02 13:23:53	Export sms	example	Success
2024-10-02 12:42:03	2024-10-02 12:42:07	Add profile: Kiosk ⓘ	system	Success
2024-10-02 12:42:02	2024-10-02 12:45:44	Policy update ⓘ	system	Success
2024-10-02 12:41:44	2024-10-02 12:41:44	Policy update ⓘ	system	Success
2024-10-02 12:41:44	2024-10-02 12:41:44	Refresh device data	system	Success

Results: 7

Page limit:

50



1



1 Filtry

- Użyj filtrów, aby wyszukać odpowiednie zadania

2 Wyczyść oczekujące zadania w aplikacji

- Ta akcja pozwala wyczyścić oczekujące zadania o statusie utworzone, anulowane lub nieudane.

3 Odśwież

- Ta akcja pozwala odświeżyć status zadań na liście zadań

4 Lista zadań

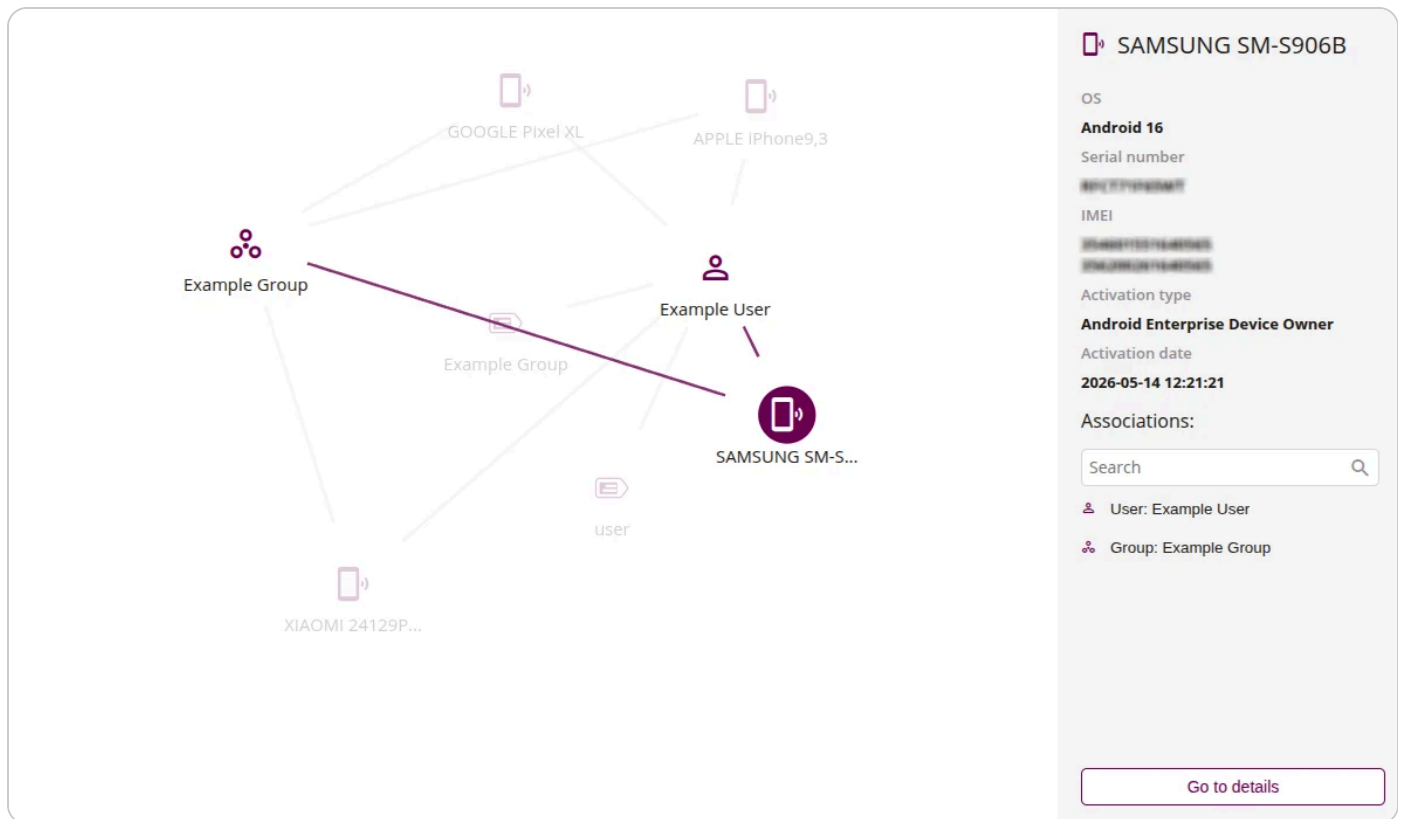
- Lista wszystkich zadań wraz z ich parametrami

Graf zależności

Zaktualizowano: 3 cze 2026

NOWOŚĆ

Zakładka Graf zależności na karcie urządzenia wyświetla interaktywną wizualizację powiązań między wybranym urządzeniem a innymi elementami systemu, takimi jak użytkownicy, grupy, role, etykiety, profile, polityki oraz integracje katalogowe (LDAP/Entra). Pozwala administratorom szybko zrozumieć, co jest przypisane lub powiązane z danym urządzeniem, bez konieczności przechodzenia między wieloma widokami.



1 Graf

- Interaktywny graf pokazujący urządzenie jako centralny węzeł z połączonymi elementami wyświetlanymi wokół niego
- Połączone elementy obejmują użytkowników, grupy, role, etykiety, profile, polityki oraz integracje katalogowe przypisane do lub powiązane z urządzeniem
- Kliknij na węzeł, aby wyświetlić jego szczegóły w panelu bocznym
- Węzły z liczbą reprezentują zagregowane elementy - kliknij, aby rozwinąć je do pojedynczych węzłów

2 Panel szczegółów

- Panel boczny wyświetlający szczegółowe informacje o wybranym elemencie
- Gdy wybrany jest węzeł urządzenia, wyświetla dane specyficzne dla urządzenia, takie jak system operacyjny, numer seryjny, IMEI, typ aktywacji i data aktywacji
- Sekcja powiązań wyświetla powiązane elementy pogrupowane w akordeony (np. Użytkownicy, Grupy, Role, Etykiety)

- Użyj pola wyszukiwania, aby filtrować powiązania
- Kliknij na element, aby przejść do szczegółowego widoku w systemie

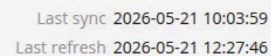
File Manager

Zaktualizowano: 3 cze 2026

BETA

Zakładka File Manager umożliwia administratorowi zdalne zarządzanie plikami na urządzeniu. Z tego widoku można przeglądać strukturę plików, tworzyć i usuwać katalogi, wgrywać i pobierać pliki oraz śledzić status zadań operacji na plikach. Funkcja działa na Androidzie (Device Owner, Profile Owner) oraz iOS (w ramach sandboxa aplikacji File Manager). Zakolejkowane akcje są wizualizowane w strukturze drzewa jako cień struktury (zielony: dodanie, czerwony: usunięcie, żółty: folder niesynchronizowany). Zadania są realizowane asynchronicznie - nawet gdy urządzenie jest offline, zostaną wykonane po przywróceniu połączenia.

Auto-refresh: None Refresh



- | | |
|--------------|---------------------|
| Example File | |
| Path | /Example File |
| Size | 9.73 MiB (10.20 MB) |
| Items | 2 |
| Modified | 2026-05-20 08:20:35 |

Files

Management

1.1 Automatyczne odświeżanie

- Wybierz z rozwijanej listy interwał automatycznego odświeżania widoku struktury plików

1.2 Odśwież

- Ta akcja pozwala odświeżyć widok struktury plików

1.3 Rozwiń wszystko

- Ta akcja pozwala rozwinąć wszystkie katalogi w drzewie plików

1.4 Zwiń wszystko

- Ta akcja pozwala zwinąć wszystkie katalogi w drzewie plików

1.5 Wymuś synchronizację struktury plików

- Ta akcja pozwala wymusić synchronizację struktury plików urządzenia z serwerem

1.6 Zleć utworzenie katalogu

- Ta akcja pozwala zlecić utworzenie nowego katalogu na urządzeniu

1.7 Prześlij plik

- Ta akcja pozwala wgrać plik z konsoli do wybranego katalogu na urządzeniu

1.8 Zleć usunięcie katalogu

- Ta akcja pozwala zlecić usunięcie wybranego katalogu na urządzeniu

1.9 Struktura plików

- Widok drzewa systemu plików urządzenia z katalogami i plikami
- Zakolejkowane akcje są widoczne w drzewie jako cień struktury (zielony: dodanie, czerwony: usunięcie, żółty: folder niezsynchronizowany)
- Kliknij prawym przyciskiem myszy na plik lub katalog, aby uzyskać dostęp do akcji kontekstowych (np. zleć usunięcie pliku, pobierz plik)

1.10 Szczegóły zaznaczonego elementu

- Panel wyświetlający szczegóły zaznaczonego pliku lub katalogu, takie jak:
 - Ścieżka
 - Rozmiar
 - Elementy
 - Data modyfikacji

2 Zadania

2.1 Filtry

- Filtry pozwalają wyszukać zadania po danych, takich jak:
 - Status
 - Typ

2.2 Anuluj zadanie

- Ta akcja pozwala anulować zadanie, które nie zostało jeszcze dostarczone do urządzenia
- Dostępne tylko dla zadań ze statusem "Oczekujące"
- Jeśli anulowane zadanie dotyczyło wgrywania pliku, powiązany plik jest również usuwany z serwera

2.3 Lista zadań

- Lista wszystkich zadań operacji na plikach i ich parametrów

3 Pliki

3.1 Filtry

- Filtry pozwalają wyszukać pliki po danych, takich jak:
 - Nazwa pliku
 - Typ

3.2 Pobierz plik

- Ta akcja pozwala pobrać plik przechowywany na serwerze na komputer

3.3 Usuń plik

- Ta akcja pozwala usunąć wybrany plik z serwera

3.4 Lista plików

- Lista wszystkich plików przechowywanych na serwerze powiązanych z tym urządzeniem i ich parametrów

4 Zarządzanie

4.1 Przegeneruj kod autoryzacji

- Ta akcja pozwala przegenerować kod autoryzacji używany przez aplikację mobilną File Manager do uwierzytelniania z serwerem
- Użyj, gdy aplikacja mobilna nie może nawiązać połączenia lub wymaga ponownej autoryzacji

Raporty

Zaktualizowano: 3 gru 2024

Tutaj możesz stworzyć raport dotyczący danych użycia urządzenia oraz znaleźć wszystkie wcześniej utworzone raporty.

Reports

Selected: 0

Deselect all

Create report

	DELIVERY DATE	ELEMENTS	PERIOD	STATUS	ISSUED BY	
✓	☐	2024-11-20 09:45:37	Mobile data usage Wi-Fi data usage Application usage Storage capacity	2024-11-20 - 2024-11-20 2024-11-20 - 2024-11-20 2024-11-20 - 2024-11-20 -	Done Done Done Done	ironman

☒ Storage capacity ☐ Mobile data usage ☐ Wi-Fi data usage ☐ Application usage

Report data:
-
Number of applications: 180
Data used: 1.48 GiB (1.59 GB)

Export report

ICON	TYPE	NAME	APPLICATION ID / P...	DATA USED	PERCENTAGE SHARE
	Application	Google	com.google.android.googl equicksearchbox	242.99 MiB (254.80 MB)	16.075
	Application	Google Play services	com.google.android.gms	148.40 MiB (155.61 MB)	9.817

1

Usuń raport

- Ta akcja pozwala na usunięcie utworzonego raportu

2

Stwórz raport

- Ta akcja pozwala na stworzenie raportu urządzenia, takiego jak:
 - Raport użycia pamięci przechowywania
 - Raport użycia danych komórkowych
 - Raport użycia danych Wi-Fi
 - Raport użycia aplikacji

3

Odśwież

- Ta akcja pozwala na odświeżenie listy raportów, jeśli wygenerowany raport nie jest wyświetlany

4 Lista raportów

- Lista wszystkich wygenerowanych raportów z urządzenia wraz z ich parametrami

Eksport

Zaktualizowano: 3 gru 2024

Tutaj możesz eksportować SMS-y, kontakty oraz listę połączeń z urządzenia oraz znaleźć wszystkie wcześniej wykonane eksporty.

Export

Date:

Type:



[Reset filters](#)

Selected: 0

[Deselect all](#)



[Export SMS](#)

[Export contacts](#)

[Export Call List](#)



☐	DATE	TYPE	SIZE
☐	2024-10-02 12:19:59	Call List	141 B
☐	2024-10-02 12:19:57	Contacts	64 B
☐	2024-10-02 12:19:55	SMS	350 B

Results: 3

Page limit:

50



1



1

Filtr eksportu

- Filtr eksportu pozwala wyszukać wyeksportowane pliki po danych, takich jak:
 - Data
 - Typ

2

Pobierz eksport

- Ta akcja pozwala pobrać wyeksportowane pliki z urządzenia

3

Usuń eksport

- Ta akcja pozwala usunąć wybrany rekord z listy eksportu

4

Eksportuj SMS

- Ta akcja pozwala wyeksportować plik SMS z urządzenia

5

Eksportuj kontakty

- Ta akcja pozwala wyeksportować plik kontaktów z urządzenia

6 Eksportuj listę połączeń

- Ta akcja pozwala wyeksportować plik listy połączeń z urządzenia

7 Odśwież

- Ta akcja pozwala odświeżyć listę eksportów

8 Lista eksportu

- Lista wszystkich wyeksportowanych plików i ich parametrów

Konta użytkownika

Zaktualizowano: 9 cze 2026

Tutaj znajdziesz listę wszystkich kont użytkownika dodanych na urządzeniu.

User accounts

Selected: 0

Deselect all



☐	NAME	TYPE
☐	Anonymous Account	al.x.grok
☐	work-862381711881474682388471134677000000@android-for-work.googleusercontent.com	com.google.work

1

Usuń

Nowość

- Ta akcja pozwala na usunięcie konta, które znajduje się na urządzeniu
- Dla niektórych kont po użyciu akcji 'Usuń' może być wymagana interakcja użytkownika na urządzeniu. Status zadania będzie wtedy zależny od akcji podjętej przez użytkownika.
- Wybrana akcja jest nieodwracalna
- Usunięcie konta Android Enterprise jest niedostępne

2

Lista kont użytkownika

- Lista wszystkich kont użytkownika dodanych na urządzeniu wraz z ich parametrami

Raporty o błędach systemowych

Zaktualizowano: 3 cze 2026

NOWOŚĆ

Zakładka Raporty o błędach systemowych umożliwia administratorowi zlecenie wygenerowania systemowego raportu błędów Android (bugreport/dumpstate) na urządzeniu. Po potwierdzeniu przez użytkownika akcji 'Udostępnij' w powiadomieniu systemowym raport jest przesyłany do serwera MDM i wyświetlany w konsoli do celów diagnostycznych. Raporty starsze niż 30 dni są automatycznie usuwane.

System bug reports

ⓘ After generating the report on your phone, **be sure to click "Share"** in the system notification. Without this, the report **will not be sent to the console**. System bug reports older than 30 days will be automatically deleted.

Completion date: From Select To Select

Status: Select

Reset filters

BASIC PQL

Selected: 0

Deselect all



Generate report



☐	COMPLETION DATE	REPORT	STATUS
☐	2026-05-15 09:10:38	System errors	Completed
☐	2026-05-15 07:42:02	System errors	Completed

1 Filtry

- Filtry pozwalają wyszukać wygenerowane raporty po danych, takich jak:
 - Data wykonania
 - Status

2 Pobierz

- Ta akcja pozwala pobrać wygenerowany plik raportu z urządzenia

3 Usuń

- Ta akcja pozwala usunąć wybrany rekord z listy raportów

4 Generuj raport

- Ta akcja pozwala zlecić urządzeniu wygenerowanie systemowego raportu błędów
 - Po kliknięciu urządzenie otrzymuje zadanie wygenerowania raportu
- Użytkownik musi potwierdzić akcję 'Udostępnij' w powiadomieniu systemowym na urządzeniu (konieczne, aby raport został wysłany do konsoli)

5 Odśwież

- Ta akcja pozwala odświeżyć listę raportów

6 Lista wygenerowanych raportów

- Lista wszystkich wygenerowanych raportów i ich parametrów
- Zaznacz raporty za pomocą checkboxów, aby wykonać zbiorczą akcję pobrania lub usunięcia

Zdjęcia z blokady

Zaktualizowano: 3 gru 2024

Tutaj znajdziesz wszystkie zdjęcia wykonane podczas blokady tego urzędu.

Photos during device lock

Date: From Select To Select

Reset filters

Selected: 0

Deselect all



☐	DATE	FILE
> ☐	2024-10-03 07:54:08	1727934848247-front.jpg
> ☐	2024-10-03 07:54:07	1727934847551-back.jpg
> ☐	2024-10-03 07:45:03	1727934303113-back.jpg
> ☐	2024-10-03 07:45:03	1727934303762-front.jpg

Results: 4



1 Filtry

- Ta funkcjonalność pozwala filtrować zdjęcia wykonane podczas blokady urządzenia według daty i nazwy pliku

2 Usun

- Ta akcja pozwala usunąć zdjęcia wykonane podczas blokady urządzenia z listy

3 Odśwież

- Ta akcja pozwala odświeżyć listę zdjęć

4 Lista zdjęć podczas blokady urządzenia

- Lista wszystkich zdjęć wykonanych podczas używania urządzenia w trakcie blokady

Użytkownicy

Zaktualizowano: 3 gru 2024

Tutaj znajdziesz listę wszystkich użytkowników, którzy zalogowali się do kiosku wraz z ich parametrami.

Users

Selected: 0

Deselect all



☐	FIRST NAME	SURNAME	USERNAME	LOGIN DATE	STATUS
☐	Example	Example	example	2024-10-03 07:49:31	Positive
☐	-	-	example user	2024-10-03 07:45:40	Positive

Results: 2

Page limit: 50

<<

<

1

>

>>

1

Pobierz

- Ta akcja pozwala pobrać dzienniki informacji o użytkownikach

2

Lista użytkowników

- Lista wszystkich użytkowników, którzy zalogowali się do kiosku wraz z ich parametrami

Grupy

Zaktualizowano: 3 gru 2024

Zakładka grupy pokazuje listę wcześniej utworzonych grup na serwerze. Grupy w systemie Proget są wykorzystywane do szybkiego i wygodnego przypisywania polityk, profili oraz aplikacji dla wielu użytkowników i urządzeń jednocześnie. Można tworzyć wiele grup z różnymi ustawieniami. Jeden użytkownik może należeć do kilku grup, pod warunkiem, że nie ma między nimi konfliktów (tzn. nie mają polityk lub profili tego samego typu).

Name: Employee X Policies: Start typing... Profiles: Start typing... Filter type: Select v

Reset filters

Selected: 0 | Deselect all     

Group priorities Add  v

☐	NAME v	POLICIES	PROFILES	APPLICATION... v	DEVICES v
☐	Employee	- Android Enterprise Profile Owner policy - Android Enterprise Device Owner policy	- ExampleActiveSyncProfile - ExampleBusinessDocumentsProfile - ExampleKioskProfile - ExampleGeofencingProfile	1	0

Results: 1 | Page limit: 50 v

  1  

1 Filtr grup

- Filtr grup pozwala na wyszukiwanie grup według danych, takich jak:
 - Nazwa
 - Polityki
 - Profile

2 Aktualizuj grupę

- Ta akcja pozwala na aktualizację grupy i przypisanie jej nowej nazwy

3 Kopiuj grupę

- Ta akcja pozwala na duplikowanie istniejących już grup w konsoli

4 Dodaj aplikacje

- Ta akcja pozwala na dodanie aplikacji dla pojedynczych lub wielu wybranych grup z listy

5 Usuń grupę

- Ta akcja pozwala na usunięcie pojedynczych lub wielu wybranych grup z listy
- Ta akcja nie jest dostępna dla grup, które są przypisane do użytkownika

6 Priorytety grup

- Ten przycisk przeniesie Cię na stronę, gdzie możesz zarządzać priorytetami grup

7 Dodaj grupę

7.1 Ustaw nazwę

- Ustaw nazwę, aby utworzyć nową grupę
- Wymagane

7.2 Powiąż z etykietą

- Stwórz etykietę, lub powiąż z istniejącą

8 Lista grup

- Lista wszystkich grup wraz z ich parametrami

8.1 Wybrana grupa

Priorytety grup

Zaktualizowano: 12 lut 2025

Group priorities

	NAME	POLICIES	PROFILES	APPLICATI...	USERS	DEVICES	
1	↕ admin	0	0	0		0	...
2	↕ user	0	0	0		1	...
3	↕ Employee	0	0	2		1	...
4	↕ testGroup	0	0	0		1	...

Back

Submit

1 Lista priorytetów grup

- Lista priorytetów grup, gdzie kolejność wskazuje na ich ważność.

Wprowadź pozycję

1 Wprowadź pozycję

- Ustaw pozycję grupy za pomocą numeru
- Wymagane

Wybrana grupa

Zaktualizowano: 3 cze 2026

Tutaj znajdziesz ogólne informacje o wybranej grupie oraz dokonasz zmian w istniejącej grupie.

Employee

Filters assigned to group

device.user.label = Employee

Group assigned profiles

- ExampleActiveSyncProfile
- ExampleBusinessDocumentsProfile
- ExampleKioskProfile
- ExampleGeofencingProfile

Group assigned policies

- Android Enterprise Device Owner policy
- Android Enterprise Profile Owner policy

Group assigned apps

Device

Container

Gmail - Email by Google

<<

<

1

>

>>

Devices assigned to group

IMEI: Start typing...

Serial number: Start typing...

User: Start typing...

+

Reset filters

MANUFACTURER	MODEL	IMEI	SERIAL NUMBER	USER	ACTIVATION TYPE
SAMSUNG	SM-G970F	XXXXXXXXXXXX	XXXXXXXXXXXX	John Doe	Android Enterprise Device Owner

Results: 1

Page limit: 50

<<

<

1

>

>>

Back

1

Edytuj nazwę grupy

- Ta akcja pozwala na edycję nazwy grupy

2

Edytuj filtr grupy

- Ta akcja pozwala na edycję filtra grupy

3 Edytuj profile grupy

- Ta akcja pozwala na edycję profili w grupie

4 Edytuj polityki grupy

- Ta akcja pozwala na edycję polityk w grupie

5 Aktualizuj aplikacje nadane przez grupę

5.1 Filtr aplikacji

- Filtr aplikacji pozwala na wyszukiwanie aplikacji, które są dodane do grupy, według danych takich jak:
 - Nazwa aplikacji
 - ID aplikacji
 - Źródło
 - Platforma

5.2 Usuń

- Ta akcja pozwala usunąć wybrane aplikacje z grupy

5.3 Globalne ustawienia dla zaznaczonych aplikacji

- Okno ustawień aplikacji pozwala skonfigurować parametry specyficzne dla platformy:
- Android
 - Tryb automatycznej instalacji (aplikacje ze sklepu)
 - Jednorazowa instalacja - aplikacja instaluje się raz; po odinstalowaniu przez użytkownika nie instaluje się ponownie
 - Wymuś instalację - aplikacja instaluje się automatycznie; po odinstalowaniu instaluje się ponownie
 - Nie instaluj - aplikacja nie jest instalowana na urządzeniu
 - Tryb automatycznej instalacji (aplikacje z plików lub zasobów zewnętrznych)
 - Wymuś instalację - aplikacja instaluje się automatycznie; po odinstalowaniu instaluje się ponownie
 - Nie instaluj - aplikacja nie jest instalowana na urządzeniu
 - Tryb automatycznej aktualizacji
 - Domyślna aktualizacja - aplikacja aktualizuje się zgodnie z domyślnymi ustawieniami

- Aktualizacja o wysokim priorytecie - aplikacja aktualizuje się automatycznie po pojawieniu się nowej wersji w Google Play
- Odroczone aktualizacje - aplikacja nie aktualizuje się automatycznie mimo dostępności nowej wersji
- Zgodnie z polityką - aplikacja aktualizuje się według założeń polityki, która znajduje się na urządzeniu
- Ustawienia odinstalowywania
 - Odinstalowanie niezablokowane - użytkownik może odinstalować aplikację
 - Odinstalowanie zablokowane - użytkownik nie może odinstalować aplikacji
 - Zgodnie z polityką - zachowanie zgodne z polityką przypisaną do urządzenia
- Wymagania połączenia Wi-Fi
 - Wi-Fi wymagane - aplikacja instaluje się/aktualizuje tylko przy połączeniu Wi-Fi
 - Wi-Fi niewymagane - aplikacja instaluje się/aktualizuje przy dowolnym połączeniu
 - Zgodnie z polityką - zachowanie zgodne z polityką przypisaną do urządzenia
- Priorytet instalacji
 - Wysoki - aplikacja z tym priorytetem instaluje się jako pierwsza w kolejce
 - Normalny - aplikacja instaluje się w standardowej kolejności
 - Niski - aplikacja z tym priorytetem zainstaluje się jako ostatnia w kolejce
- Instaluj tylko w stanie bezczynności - instalacja odbywa się tylko gdy urządzenie nie jest używane
 - Tak
 - Nie
- Instaluj tylko podczas ładowania - instalacja odbywa się tylko gdy urządzenie jest podłączone do ładowarki
 - Tak
 - Nie
- Powiadom użytkownika po przypisaniu konfiguracji aplikacji - wyświetla powiadomienie po przypisaniu nowej konfiguracji
 - Tak

- Nie
- Wyczyść dane aplikacji przed przypisywaniem konfiguracji - usuwa istniejące dane aplikacji przed zastosowaniem nowej konfiguracji
 - Tak
 - Nie
- Apple
 - Wymagana
 - Tak - aplikacja jest wymagana na urządzeniu i instalowana automatycznie
 - Nie - aplikacja nie jest wymagana, użytkownik może ją zainstalować opcjonalnie
 - Profil
 - Lista dostępnych profili konfiguracyjnych do przypisania aplikacji
 - Brak
 - Opcje zarządzania
 - Brak - Brak ustawienia
 - Usuń aplikację - Jeśli aplikacja została zainstalowana jako zarządzana, zostanie usunięta po usunięciu profilu MDM
 - Zablokuj tworzenie kopii zapasowych - Zapobiega tworzeniu kopii zapasowej danych aplikacji
 - Usuń aplikację i zablokuj tworzenie kopii zapasowych - Łączy obie funkcje: usuwa aplikację po usunięciu profilu MDM i blokuje tworzenie kopii zapasowych
 - Konwertuj z trybu niezależnego na zarządzany - przejęcie kontroli nad aplikacją zainstalowaną wcześniej przez użytkownika
 - Tak
 - Nie
 - Możliwość zablokowania - pozwala zablokować aplikację na ekranie urządzenia (Funkcja dostępna od iOS 18)
 - Tak
 - Nie
 - Możliwość ukrycia - pozwala ukryć ikonę aplikacji

- Tak
- Nie
- Funkcja dostępna tylko gdy 'Możliwość zablokowania jest włączona'
- Możliwość usunięcia - pozwala użytkownikowi odinstalować aplikację
 - Tak
 - Nie
- Blokada ekranu dla Tap to Pay - wymusza blokadę ekranu po transakcji Tap to Pay
 - Tak
 - Nie
- Włącz bezpośrednie pobieranie dla powiązanych domen
 - Tak
 - Nie
- Zarządzaj powiązanymi domenami
 - Dodaj
 - Usuń
- Powiązane domeny (lista domen w formacie applinks:example.com)
 - Dostępne jeśli jest wybrana opcja 'Dodaj' w 'Zarządzaj powiązanymi domenami'

5.4 Dodaj aplikacje

- Przypisz aplikacje do grupy

5.5 Konfiguruj pojedynczą aplikację

- Okno konfiguracji aplikacji pozwala ustawić parametry specyficzne dla platformy:
- Android
 - Tryb automatycznej instalacji (aplikacje ze sklepu)
 - Tryb automatycznej instalacji (aplikacje z plików lub zasobów zewnętrznych)
 - Tryb automatycznej aktualizacji

- Ustawienia odinstalowania
- Wymagania połączenia Wi-Fi
- Priorytet instalacji
- Instaluj tylko gdy bezczynne - instalacja odbywa się tylko gdy urządzenie nie jest używane
- Instaluj tylko podczas ładowania - instalacja odbywa się tylko gdy urządzenie jest podłączone do ładowarki
- Powiadom użytkownika po przypisaniu konfiguracji aplikacji - wyświetla powiadomienie po przypisaniu nowej konfiguracji
- Wyczyść dane aplikacji przed przypisaniem konfiguracji - usuwa istniejące dane aplikacji przed zastosowaniem nowej konfiguracji
- Wersja aplikacji - umożliwia wybór konkretnej wersji aplikacji do zainstalowania na urządzeniu
- Konfiguracja aplikacji - pozwala przypisać dodatkowe parametry konfiguracyjne aplikacji (np. managed app configuration)
- Apple
 - Wymagane
 - Wersja aplikacji - umożliwia wybór konkretnej wersji aplikacji do zainstalowania na urządzeniu
 - Profil
 - Konfiguracja aplikacji - pozwala przypisać dodatkowe parametry konfiguracyjne aplikacji (np. managed app configuration)
 - Opcje zarządzania
 - Konwertuj z niezarządzanej na zarządzaną - przejęcie kontroli nad aplikacją wcześniej zainstalowaną przez użytkownika
 - Możliwa do zablokowania - pozwala zablokować aplikację na ekranie urządzenia (Funkcja dostępna od iOS 18)
 - Możliwa do ukrycia - pozwala ukryć ikonę aplikacji
 - Możliwa do usunięcia - pozwala użytkownikowi odinstalować aplikację
 - Blokada ekranu dla Tap to Pay - wymusza blokadę ekranu po transakcji Tap to Pay
 - Włącz bezpośrednio pobieranie dla powiązanych domen
 - Zarządzaj powiązanymi domenami

- Powiązane domeny (lista domen w formacie applinks:example.com)

6 Lista urządzeń

- Lista wszystkich urządzeń dodanych do grupy, wraz z ich parametrami

Zarządzaj filtrem

Zaktualizowano: 16 lip 2026

Zarządzanie filtrem grupy umożliwia w różny sposób przypisywanie grup do wybranych urządzeń

Manage filter of the group EmployeeNEW

 Give feedback

Select:

☐ No devices

☐ All devices

☒ Custom settings

 Specify conditions for adding devices to a group using PQL syntax. Go to the [knowledge base](#) to find out more.

device.user.label = EmployeeX

 Saved filters▼

Results: 1

BackSubmit

MANUFACTURER	MODEL	USER
SAMSUNG	SM-G970F	John Doe

Results: 1 | Page limit: 50▼

<<<1>>>

1 Bez urządzeń

- Wybrany filtr nie przypisze grupy do żadnego urządzenia

2 Wszystkie urządzenia

- Wybrany filtr przypisze grupę do wszystkich urządzeń w systemie oraz tych, które będą do niego wdrażane

3 Ustawienia własne

- Wybrany filtr umożliwia wpisanie własnego filtra PQL

4 Pole filtra

- Filtr PQL umożliwia wyszukiwanie urządzeń już dodanych do systemu i tych, które zostaną dodane na podstawie danych:
 - IMEI
 - Numer seryjny
 - Proget ID
 - Producent
 - Model
- Maksymalna długość zapytania: 4000
- Maksymalna liczba warunków: 50
- Wymagane

5 Zapisane filtry

- Ta akcja umożliwia wybranie z listy filtra, który jest już utworzony w systemie

6 Liczba urządzeń

- Lista wszystkich urządzeń wraz z ich parametrami, do których zostaną dodane grupy

Język zapytań Proget (PQL)

Zaktualizowano: 3 cze 2026

Proget Query Language (PQL) to prosty język zapytań, który umożliwia filtrowanie urządzeń w systemie. Dzięki PQL możesz dynamicznie przypisywać urządzenia do grup na podstawie zdefiniowanych kryteriów, tworząc tzw. grupy dynamiczne. Wcześniej grupy były statyczne – administratorzy ręcznie przypisywali urządzenia do grup. Teraz, dzięki PQL, grupy mogą automatycznie obejmować urządzenia spełniające określone warunki, takie jak dane urządzeń lub etykiety użytkowników. Możliwe jest również łączenie różnych kryteriów w ramach jednego zapytania. Dynamiczne grupowanie pozwala na wstępne przygotowanie konfiguracji, która zostanie automatycznie przypisana do urządzeń, nawet jeśli jeszcze nie są one obecne w systemie. Konfiguracja może być modyfikowana na podstawie atrybutów użytkowników pobranych z zewnętrznych katalogów, takich jak Active Directory. Wprowadzone zmiany w katalogu mogą automatycznie wpływać na konfigurację urządzeń w systemie Proget. Dzięki PQL możliwe jest łatwe tworzenie grup urządzeń, bez konieczności ręcznego przypisywania. Jeżeli nie korzystasz z zaawansowanych funkcji PQL, domyślny mechanizm tworzenia grup automatycznie utworzy etykietę dla danej grupy. Aby uzyskać zgodność z poprzednimi wersjami systemu, wystarczy przypisać użytkownikowi etykietę o tej samej nazwie, co grupa.

Manage filter of the group Employee

Select:

☐ No devices

☒ All devices

☐ Custom settings

All devices will be assigned to this group
Results: 2

Back

Submit

1 Brak urządzeń

- Pusta grupa, do której nie zostaną przypisane żadne urządzenia

2 Wszystkie urządzenia

- Automatycznie obejmuje wszystkie urządzenia w systemie

- Umożliwiają tworzenie filtrów PQL na podstawie określonych kryteriów
-

Ustawienia niestandardowe

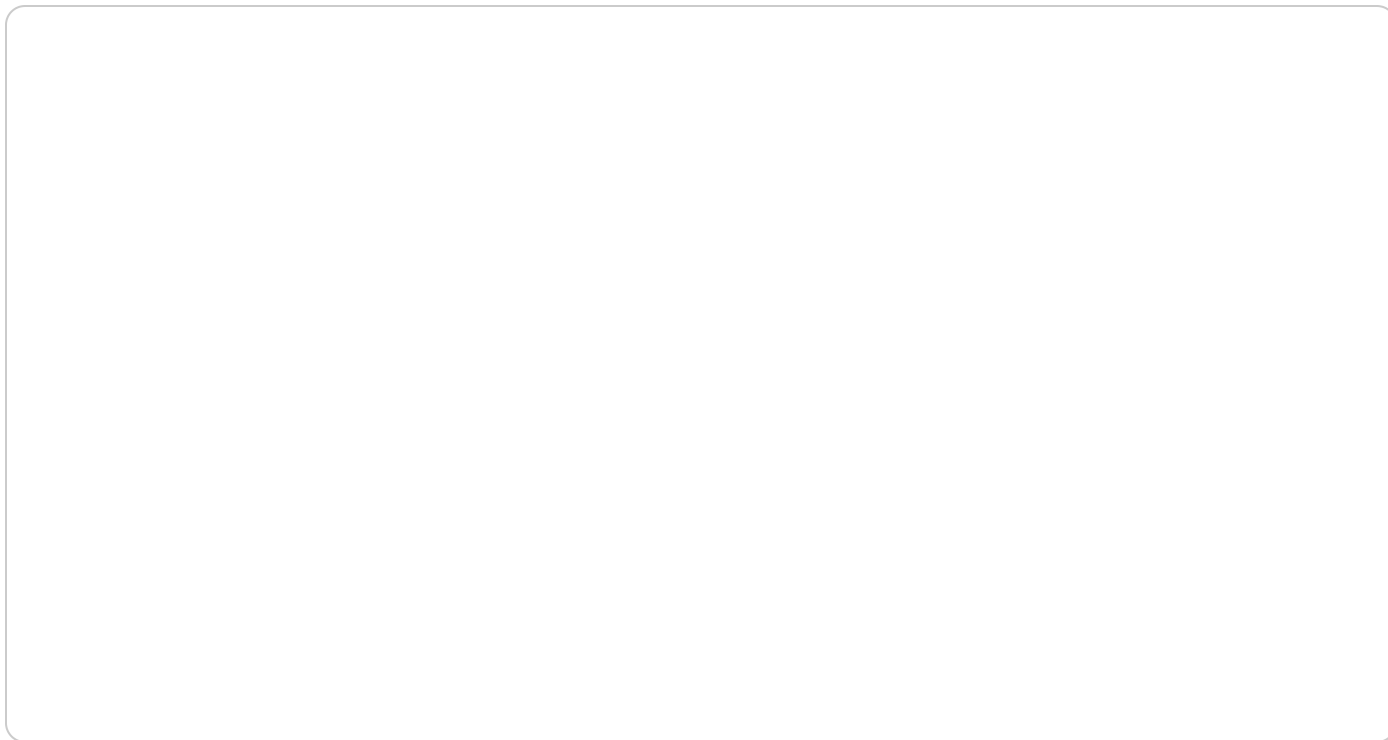
W sekcji 'Ustawienia niestandardowe' administrator może tworzyć filtry PQL, korzystając z dostępnych parametrów. System podpowiada dostępne opcje podczas pisania, co czyni tworzenie zapytań intuicyjnym. Gdy składnia jest poprawna, administrator może zobaczyć listę urządzeń spełniających warunki filtru, co ułatwia bieżącą weryfikację wyników.

Aby lepiej zrozumieć składnię filtrów, przedstawiamy kilka podstawowych pojęć:

Kluczowe elementy filtru PQL

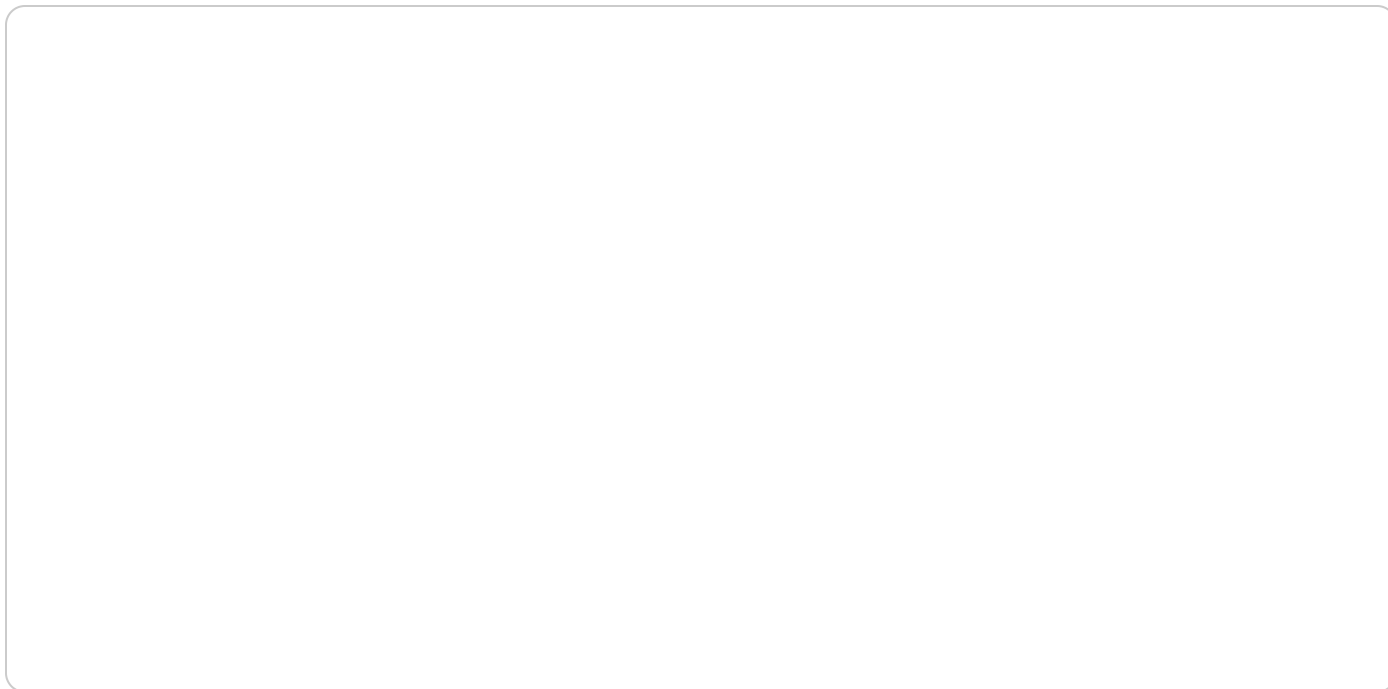
- **Fraza**
 - Pojedyncze wyrażenie składające się z *parametru*, *operatora* i *wartości*
 - Każdy filtr musi zawierać co najmniej jedną frazę
 - Frazy można łączyć za pomocą operatorów logicznych (*AND*, *OR*)
 - **Parametr**
 - Określa atrybut urządzenia lub jego właściciela, który jest filtrowany
 - **Operator**
 - Łączy *parametr* z *wartością* i określa relację między nimi
 - **Wartość**
 - Prawa strona wyrażenia, określająca, czego szukamy (np. tekst, liczba, wartość logiczna)
 - **Łącznik**
 - Łączy frazy w bardziej złożone zapytania
 - Dostępne łączniki: *AND*, *OR*
-

Przykłady filtrów



1 **device.os.type = android**

- Ten filtr przypisuje do grupy wszystkie urządzenia z systemem operacyjnym Android



1 device.user.label != Pracownik

- Ten filtr obejmuje wszystkie urządzenia, których właściciel nie ma etykiety "Pracownik"

1 device.user.organizationUnit contains Office AND device.user.isBlocked = false AND device.os.type = android

- Ten filtr łączy kilka kryteriów:
 - Urządzenie należy do użytkownika, którego jednostka organizacyjna (wartość synchronizowana z usługą katalogową) zawiera w nazwie słowo 'Office'
 - Użytkownik urządzenia nie jest zablokowany w systemie Proget
 - Urządzenie działa na systemie Android

Klucze

Klucz	Dostępne operatory	Typ wartości	Opis
device.manufacturer	<i>=, !=, in, not_in</i>	wyliczeniowy	Producent urządzenia, np. Samsung
device.model	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with, in, not_in</i>	wyliczeniowy	Model urządzenia, np. <i>iPhone 13</i>
device.serialNumber	<i>=, !=</i>	tekst	Numer seryjny urządzenia
device.progetId	<i>=, !=</i>	tekst	Proget ID urządzenia, np. <i>123 456</i>
device.os.type	<i>=, !=</i>	wyliczeniowy	System operacyjny urządzenia np. <i>Android</i>
device.os.versionCode	<i>=, !=, >, >=, <, <=</i>	liczba	Wersja systemu operacyjnego urządzenia np. <i>33</i> (Android 13)
device.activationType	<i>=, !=</i>	wyliczeniowy	Rodzaj aktywacji np. <i>android_mdm</i>
device.systemUpdateStatus	<i>=, !=</i>	wyliczeniowy	Wartość ze zdefiniowanego zbioru np. <i>available</i>
device.SIM1.IMEI	<i>=, !=</i>	tekst	IMEI dla SIM1
device.SIM2.IMEI	<i>=, !=</i>	tekst	IMEI dla SIM2
device.SIM1 NOWOŚĆ	<i>=, !=</i>	wyliczeniowy	Określa, czy w slotie 1 jest karta SIM. Użyj

			wartości << <i>Brak</i> >>, aby sprawdzić, czy slot jest pusty
device.SIM2 NOWOŚĆ	=, !=	wyliczeniowy	Określa, czy w slotie 2 jest karta SIM. Użyj wartości << <i>Brak</i> >>, aby sprawdzić, czy slot jest pusty
device.SIM1.ICCID	=, !=, <i>in</i> , <i>not_in</i>	tekst	ICCID dla SIM1
device.SIM2.ICCID	=, !=, <i>in</i> , <i>not_in</i>	tekst	ICCID dla SIM2
device.SIM1.carrier	=, !=	tekst	Operator SIM1
device.SIM2.carrier	=, !=	tekst	Operator SIM2
device.mdmVersionCode	=, !=, >, >=, <, <=	liczba	Wersja kodowa aplikacji Proget
device.alias	=, !=, <i>contains</i> , <i>not_contains</i> , <i>starts_with</i> , <i>not_starts_with</i> , <i>ends_with</i> , <i>not_ends_with</i>	tekst	Alias urządzenia
device.user	=, !=, <i>in</i> , <i>not_in</i>	tekst	Urządzenie należące do użytkownika np. « Brak », <i>John Doe</i> - <i>jdoe@example.com</i> (UUID)
device.user.uuid	=, !=	tekst	UUID użytkownika
device.user.isBlocked	=, !=	logiczna	Urządzenie należące do zablokowanego użytkownika

device.user.email	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Email użytkownika np. <i>jdoe@example.com</i>
device.user.type	<i>=, !=</i>	wyliczeniowy	Typ użytkownika np. <i>lokalny</i>
device.user.displayName	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Imię i nazwisko użytkownika np. <i>John Doe</i>
device.user.username	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Nazwa użytkownika np. <i>jdoe</i>
device.user.principalName	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Email użytkownika np. <i>jdoe@example.com</i>
device.user.title	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Tytuł użytkownika

device.user.distinguishedName	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Nazwa wyróżniająca użytkownika (<i>DN</i>)
device.user.commonName	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Nazwa zwyczajowa użytkownika
device.user.country	<i>=, !=</i>	tekst	Kraj użytkownika
device.user.organization	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Organizacja użytkownika
device.user.organizationUnit	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Oddział organizacji użytkownika
device.user.locality	<i>=, !=</i>	tekst	Lokalizacja
device.user.title	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Tytuł użytkownika

device.user.label	<i>=, !=, in, not_in</i>	tekst	Etykieta użytkownika
device.user.directoryGroup	<i>=, !=, in, not_in</i>	tekst	Grupa katalogowa użytkownika
device.user.customAttribute1	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Custom attribute 1
device.user.customAttribute2	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Custom attribute 2
device.user.customAttribute3	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Custom attribute 3
device.user.customAttribute4	<i>=, !=, contains, not_contains, starts_with, not_starts_with, ends_with, not_ends_with</i>	tekst	Custom attribute 4

Referencje

Referencja	Używana z kluczami	Dostępne operatory	Opis
ALLOWED_SIM_CARDS NOWOŚĆ	<i>device.SIM1.ICCID,</i> <i>device.SIM2.ICCID</i>	<i>in, not_in</i>	Lista dozwolonych kart SIM (ICCID) zarządzana w <i>Ustawienia → Dozwolone karty SIM</i>

Operatory

- **=** - porównanie (równa się)
- **!=** - porównanie (nie równa się)
- **<** - porównanie (mniejszy)
- **<=** - porównanie (mniejszy lub równy)
- **>** - porównanie (większy)
- **>=** - porównanie (większy lub równy)
- **contains** - zawiera określony fragment tekstu
- **not_contains** - nie zawiera określonego fragmentu tekstu
- **starts_with** - zaczyna się od określonego fragmentu tekstu
- **not_starts_with** - nie zaczyna się od określonego fragmentu tekstu
- **ends_with** - kończy się określonym fragmentem tekstu
- **not_ends_with** - nie kończy się określonym fragmentem tekstu
- **in** - zawiera określone wartości
- **not_in** - nie zawiera określonych wartości

Typy wartości

- **tekst** - np. 'SAMSUNG'. Wartości wielowyrazowe należy umieszczać w cudzysłowie
- **liczba** - np. liczba całkowita lub zmiennoprzecinkowa
- **logiczna** - wartość logiczna *true* lub *false*
- **wyliczeniowa** - wartość ze zdefiniowanego zbioru, np. typ systemu operacyjnego
- **referencja** - odwołanie do predefiniowanej listy zarządzanej w innym miejscu systemu, np. *ALLOWED_SIM_CARDS* odwołujące się do listy dozwolonych kart SIM

Aplikacje

Zaktualizowano: 16 lip 2026

W zakładce Aplikacje znajdziesz tabelę z informacjami o aplikacjach na danym serwerze.

App name: Start typing...Package Id: pl.progetXOrigin: SelectPlatform: Select

Reset filters

Selected: 0 | Deselect all

Add

ICON	APP NAME	PACKAGE ID	ORIGIN	PLATFO...
☐	 Proget	pl.proget.progetmdm	Store	Android 
☐	 Proget Backup	pl.proget.backup	Store	Android 
☐	 Proget Backup From File Version: master (33)	pl.proget.backup	File ⓘ	Android 
☐	 Proget Filesharing Version: 1.5.0 (14)	pl.proget.filesharing	File ⓘ	Android 
☐	 Proget File Sharing	pl.proget.filesharing	Store	Android 
☐	 Proget Geofencing	pl.proget.geofencing	Device	Android
☐	 Proget OpenVPN	pl.proget.openvpn	Store	Android 
☐	 Proget Remote	pl.proget.remote	Store	Android 

Results: 8 | Page limit: 50

1 Filtrowanie w oknie tekstowym

- Możesz filtrować wyniki, używając słów kluczowych. Wprowadź słowo kluczowe, które chcesz użyć do filtrowania, w odpowiednie pole. Wyniki są filtrowane dynamicznie podczas wpisywania tekstu.

2 Aktualizacja reguł

2.1 Dostępne reguły

- Wybierz jedną z dostępnych reguł
- Wymagane

2.2 Android Enterprise - przestrzeń robocza

- Ta akcja pozwala dodać wybraną aplikację do reguł Android Enterprise - przestrzeń robocza, takich jak:
 - Brak
 - Odblokuj aplikacje
 - Czarna lista

2.3 Android Enterprise - przestrzeń prywatna

- Ta akcja pozwala dodać wybraną aplikację do reguł Android Enterprise - przestrzeń prywatna, takich jak:
 - Brak
 - Biała lista
 - Czarna lista

2.4 iOS (tryb nadzorowany)

- Ta akcja pozwala dodać wybraną aplikację do reguł iOS (tryb nadzorowany), takich jak:
 - Brak
 - Biała lista
 - Czarna lista

3 Synchronizacja ze sklepem

- Ta akcja pozwala na synchronizację wybranych aplikacji ze sklepem

4 Usun aplikację

- Ta akcja pozwala usunąć wybrane aplikacje

5 Dodaj aplikację

- Po kliknięciu przycisku zostaniesz przeniesiony do zakładki, gdzie możliwe jest dodanie aplikacji do konsoli Proget

6 Lista aplikacji

- Lista wszystkich aplikacji dodanych do konsoli Proget ze sklepu lub z pliku

6.1 Pojedyncza aplikacja Android

6.2 Pojedyncza aplikacja Android z pliku

6.3 Pojedyncza aplikacja iOS

Dodaj aplikacje

Zaktualizowano: 21 mar 2025

Tutaj możesz dodać aplikacje do konsoli Proget z pliku, z Google Play lub z iTunes.

Add application

☐

From the file

☐

From the external resource ⓘ

☐

Google Play

☐

iTunes

Back

1 Dodaj aplikacje z pliku

1.1 Nazwa

- Wprowadź nazwę aplikacji

1.2 Opis

- Wprowadź opis aplikacji

1.3 Wybierz plik

- Wybierz aplikację z pliku
- Dozwolony typ pliku: .apk, .ipa, .pkg
- Maksymalny rozmiar przesyłanych plików to 314,52 MB (300,00 MiB)

2

Dodawanie aplikacji z zewnętrznego zasobu

2.1 Nazwa

- Wprowadź nazwę aplikacji
- Maksymalna długość tekstu to 255
- Wymagane

2.2 ID aplikacji

- Wprowadź ID aplikacji
- Maksymalna długość tekstu to 255
- Wymagane

2.3 URL

- Wprowadź link URL do zewnętrznego zasobu, w którym znajduje się aplikacja
- Maksymalna długość tekstu to 255
- Wymagane

2.4 Suma kontrolna

- Wprowadź sumę kontrolną aplikacji
- Suma kontrolna jest używana do sprawdzania, czy plik APK jest nienaruszony. Jest uzyskiwana poprzez konwersję pliku APK na format Base64, a następnie obliczenie jego wartości skrótu SHA-256. W celu uzyskania szczegółowych instrukcji przejdź do bazy wiedzy.
- Wymagane

2.5 Wersja

- Wprowadź wersję aplikacji
- Maksymalna długość tekstu to 255

- Wymagane

2.6 Kod wersji

- Wprowadź kod wersji aplikacji
- Maksymalna wartość to 2100000000
- Wymagana liczba

2.7 Wymagane uwierzytelnienie

- Sprawdź, czy wymagane jest uwierzytelnienie dostępu do zewnętrznego zasobu
- Jeśli zaznaczone, wymagane jest wprowadzenie loginu i hasła

2.8 Login

- Wprowadź login, którego używasz do logowania się do zewnętrznego zasobu

2.9 Hasło

- Wprowadź hasło, którego używasz do logowania się do zewnętrznego zasobu

2.10 Opis

- Możesz wprowadzić opis aplikacji
- Maksymalna długość tekstu to 255

2.11 Wybierz plik

- Możesz ustawić własną ikonę dla aplikacji z zewnętrznego zasobu

2.12 Usuń

- Usuń wybraną ikonę dla aplikacji z zewnętrznego zasobu

3 Dodaj aplikacje z Google Play

3.1 Google Play

- Tutaj możesz wyszukać aplikację w sklepie Google Play i dodać ją do konsoli Proget

4 Dodaj aplikacje z iTunes

4.1 iTunes

- Tutaj możesz wyszukać aplikację w sklepie iTunes i dodać ją do konsoli Proget

Pojedyncza aplikacja Android

Zaktualizowano: 16 paź 2025

Tutaj znajdziesz informacje o pojedynczej aplikacji, takie jak: ID aplikacji, źródło, platforma, urządzenia z zastosowaną konfiguracją, App config feedback oraz wersje aplikacji. Możesz również wykonywać akcje na aplikacji i konfigurować ustawienia, takie jak: konfiguracja aplikacji i uprawnienia aplikacji.

 **Gmail**



Package Id:

com.google.android.gm

Origin:

Store

Platform:

android

 **Description**
Connect, create and collaborate with Gmail, part of Google Workspace.

Configuration

Devices

App config feedback

Runtime permissions

Versions

Selected: 0

Deselect all



Add configuration

☐	CONFIGURATION N...	GROUPS	CREATION DATE	MODIFICATION DATE	CREATED BY	MODIFIED BY
☐	Example configuration	-	2025-02-11 12:53:57	2025-02-11 12:54:57	Example user	Example user

1 Przejdź do szczegółów w sklepie

- Po kliknięciu tego przycisku zostaniesz przeniesiony do szczegółów aplikacji w witrynie sklepu Google Play

2 Synchronizacja ze sklepem

- Po kliknięciu tego przycisku aplikacja zostanie zsynchronizowana ze sklepem

3 Aktualizacja reguł

3.1 Dostępne reguły

- Wybierz jedną z reguł aplikacji w profilu
- Wymagane

3.2 Android Enterprise - przestrzeń robocza

- Ta akcja pozwala dodać wybraną aplikację do reguł Android Enterprise - przestrzeń robocza, takich jak:
 - Brak
 - Odblokuj aplikacje
 - Czarna lista

3.3 Android Enterprise - przestrzeń prywatna

- Ta akcja pozwala dodać wybraną aplikację do reguł Android Enterprise - przestrzeń prywatna, takich jak:
 - Brak
 - Biała lista
 - Czarna lista

3.4 iOS (tryb nadzorcy)

- Ta akcja pozwala dodać wybraną aplikację do reguł iOS (tryb nadzorcy), takich jak:
 - Brak
 - Biała lista
 - Czarna lista

4 Usuń aplikację

- Ta akcja pozwala usunąć aplikację z konsoli Proget

5 Konfiguracja

5.1 Edytuj konfigurację

- Ta akcja pozwala edytować konfigurację aplikacji

5.2 Aktualizuj konfigurację

- Ta akcja pozwala zaktualizować konfigurację aplikacji

5.3 Kopiuj konfigurację

- Ta akcja pozwala na skopiowanie konfiguracji aplikacji

5.4 Usuń konfigurację

- Ta akcja pozwala usunąć konfigurację aplikacji

5.5 Dodaj konfigurację

- Ta akcja pozwala dodać konfigurację aplikacji

5.6 Lista konfiguracji

- Lista konfiguracji aplikacji

6 Urządzenia

6.1 Wyczyść dane

- Ta akcja pozwala wyczyścić dane wybranej aplikacji na wszystkich urządzeniach, na których jest zainstalowana

6.2 Zablokuj

- Ta akcja pozwala zablokować wybraną aplikację na wszystkich urządzeniach, na których jest zainstalowana

6.3 Odblokuj

- Ta akcja pozwala odblokować wybraną aplikację na wszystkich urządzeniach, na których jest zainstalowana

6.4 Uruchom

- Ta akcja pozwala uruchomić wybraną aplikację na wszystkich urządzeniach na których jest zainstalowana

6.5 Wyślij konfigurację

- Ta akcja pozwala wysłać konfigurację wybranej aplikacji na wszystkie urządzenia, na których jest zainstalowana

6.6 Usuń

- Ta akcja pozwala usunąć wybraną aplikację ze wszystkich urządzeń, na których jest zainstalowana

6.7 Eksport

- Ta akcja pozwala eksportować listę urządzeń wraz z informacjami o między innymi: modelu, użytkowniku, statusie urządzenia, wersji zainstalowanej aplikacji itd

6.8 Ustawienia tabeli

- W ustawieniach tabeli możesz wybrać, które kolumny będą wyświetlane

6.9 Lista urządzeń

- Lista urządzeń wraz z informacjami o między innymi: modelu, użytkowniku, statusie urządzenia, wersji zainstalowanej aplikacji itd

7 Opinie o konfiguracji aplikacji

7.1 Lista opinii o konfiguracji aplikacji

- Lista opinii o konfiguracji aplikacji wraz z informacjami o statusie i urządzeniach

8 Uprawnienia aplikacji

8.1 Uprawnienia aplikacji

- Uprawnienia aplikacji, gdzie możesz zmienić sposób ich przydzielania, takich jak:
 - Pytaj użytkownika
 - Automatycznie przydziel
 - Automatycznie odrzuć

9 Wersje

9.1 Lista wersji

- Lista wersji wraz z ich ilością na urządzeniu i w kontenerze

Pojedyncza aplikacja Android z pliku

Zaktualizowano: 11 lut 2025

Tutaj znajdziesz informacje o pojedynczej aplikacji, takie jak: ID aplikacji, źródło, platforma, urządzenia z zastosowaną konfiguracją, App config feedback oraz wersje aplikacji. Możesz również wykonywać akcje na aplikacji i konfigurować ustawienia, takie jak: konfiguracja aplikacji i uprawnienia aplikacji.

 **Proget File Sharing**



Package Id:
pl.proget.filesharing

Origin:
File

Platform:
android

Version:
1.5.1

Version code:
15

Size:
9.73 MiB (10.20 MB)

Devices

App config feedback

Runtime permissions

Versions

IMEI:

Serial number:

User:

Version:



Selected: 0 | Deselect all



☐	MANUFACTURER ▾	MODEL ▾	USER ▾	DEVICE STATUS ▾	VERSION ▾
☐	SAMSUNG	SM-T580	-	Active	master

Results: 1 | Page limit:



1

Aktualizacja aplikacji

1.1 Wybierz plik

- Ta akcja pozwala na aktualizację aplikacji z pliku, poprzez przesłanie nowszej wersji aplikacji z Twojego urządzenia

1.2 Zamknij

- Ta akcja pozwala zamknąć okno dialogowe aktualizacji aplikacji

1.3 Aktualizuj

- Ta akcja pozwala zaktualizować aplikację z pliku do nowszej wersji

2 Pobierz aplikację

- Ta akcja pozwala na pobranie aplikacji na Twoje urządzenie

3 Aktualizacja reguł

3.1 Dostępne reguły

- Wybierz jedną z reguł aplikacji w profilu
- Wymagane

3.2 Android Enterprise - przestrzeń robocza

- Ta akcja pozwala dodać wybraną aplikację do reguł Android Enterprise - przestrzeń robocza, takich jak:
 - Brak
 - Odblokuj aplikacje
 - Czarna lista

3.3 Android Enterprise - przestrzeń prywatna

- Ta akcja pozwala dodać wybraną aplikację do reguł Android Enterprise - przestrzeń prywatna, takich jak:
 - Brak
 - Biała lista
 - Czarna lista

3.4 iOS (tryb nadzorcy)

- Ta akcja pozwala dodać wybraną aplikację do reguł iOS (tryb nadzorcy), takich jak:
 - Brak
 - Biała lista
 - Czarna lista

4 Schemat konfiguracji

4.1 Schemat

- Wprowadź schemat konfiguracji JSON lub przeciągnij i upuść plik tutaj dla wybranej aplikacji z pliku, która może być skonfigurowana

4.2 Formatuj JSON

- Ta akcja pozwala na sformatowanie schematu konfiguracji JSON

4.3 Anuluj

- Ta akcja pozwala na przerwanie konfiguracji schematu

4.4 Zapisz

- Ta akcja pozwala zapisać wprowadzoną konfigurację schematu

5 Usuń aplikację

- Ta akcja pozwala usunąć aplikację z konsoli Proget

6 Urządzenia

6.1 Wyczyść dane

- Ta akcja pozwala wyczyścić dane wybranej aplikacji na wszystkich urządzeniach, na których jest zainstalowana

6.2 Uruchom

- Ta akcja pozwala uruchomić wybraną aplikację na wszystkich urządzeniach na których jest zainstalowana

6.3 Usuń

- Ta akcja pozwala usunąć wybraną aplikację ze wszystkich urządzeń, na których jest zainstalowana

6.4 Eksport

- Ta akcja pozwala eksportować listę urządzeń wraz z informacjami o między innymi: modelu, użytkowniku, statusie urządzenia, wersji zainstalowanej aplikacji itd

6.5 Ustawienia tabeli

- W ustawieniach tabeli możesz wybrać, które kolumny będą wyświetlane

6.6 Lista urządzeń

- Lista urządzeń z informacjami o między innymi: modelu, użytkowniku, statusie urządzenia, wersji zainstalowanej aplikacji itd

7 Opinie o konfiguracji aplikacji

7.1 Lista opinii o konfiguracji aplikacji

- Lista opinii o konfiguracji aplikacji wraz z informacjami o statusie i urządzeniach

8 Uprawnienia aplikacji

8.1 Uprawnienia aplikacji

- Uprawnienia aplikacji, gdzie możesz zmienić sposób ich przydzielania, takie jak:
 - Pytaj użytkownika
 - Automatycznie przydziel
 - Automatycznie odrzuć

9 Wersje

9.1 Lista wersji

- Lista wersji wraz z ich ilością na urządzeniu i w kontenerze

10 Eksport

- Ta akcja pozwala wyeksportować listę urządzeń z informacjami o modelu, użytkowniku, statusie urządzenia i wersji zainstalowanej aplikacji

11 Ustawienia tabeli

- W ustawieniach tabeli możesz wybrać, które kolumny będą wyświetlane

Pojedyncza aplikacja iOS

Zaktualizowano: 9 lip 2025

Tutaj znajdziesz informacje o pojedynczej aplikacji, takie jak: ID pakietu, pochodzenie i platforma. Możesz również dodać konfigurację aplikacji.

 SinglelosApp



Package Id:	Origin:	Platform:	Version:	Version code:	Size:
com.petri.calculator.calculator	File	ios	1.0	0	21.18 MiB (22.21 MB)

Configuration

Selected: 0 | Deselect all



Add configuration

☐	CONFIGURATION ...	GROUPS	CREATION DATE	MODIFICATION D...	CREATED BY	MODIFIED BY
☐	Example configuration	-	2025-07-08 13:00:21	2025-07-08 13:03:57	Example Example	Example Example

- 1

Aktualizuj aplikację
- Po kliknięciu tego przycisku będziesz mógł zaktualizować aplikację, wybierając bieżącą wersję ze swojego urządzenia
- 2

Pobierz aplikację
- Po kliknięciu tego przycisku aplikacja zostanie pobrana na twoje urządzenie
- 3

Dodaj do reguły

3.1 Dostępne reguły

- Wybierz jedną z dostępnych reguł
- Wymagane

3.2 Android Enterprise - przestrzeń robocza

- Ta akcja pozwala dodać wybraną aplikację do reguł Android Enterprise - przestrzeń robocza, takich jak:
 - Brak
 - Odblokuj aplikacje
 - Czarna lista

3.3 Android Enterprise - przestrzeń prywatna

- Ta akcja pozwala dodać wybraną aplikację do reguł Android Enterprise - przestrzeń prywatna, takich jak:
 - Brak
 - Biała lista
 - Czarna lista

3.4 iOS (tryb nadzorowany)

- Ta akcja pozwala dodać wybraną aplikację do reguł iOS (tryb nadzorowany), takich jak:
 - Brak
 - Biała lista
 - Czarna lista

4 Usunąć aplikację

- Ta akcja pozwala usunąć aplikację z konsoli Proget

5 Dodaj konfigurację

- Ta akcja pozwala dodać konfigurację aplikacji

6 Konfiguracja

- Lista konfiguracji aplikacji

Polityki

Zaktualizowano: 16 lip 2026

Polityki w systemie Proget pozwalają łatwo ograniczyć dostęp użytkowników do funkcji dostępnych na urządzeniach mobilnych. Dzięki politykom możemy, dla wybranej grupy urządzeń, narzucić pożądaną złożoność hasła, ograniczyć korzystanie z aparatu lub zabronić korzystania z usług Google. Polityki są grupowane według rodzaju aktywacji. Znajdziesz także predefiniowane domyślne polityki, które są kompatybilne z aktywacjami urządzeń.



Android Enterprise Device Owner

Zasady haseł, aplikacji, bezpieczeństwa i lokalizacji dla Device Owner



Android Enterprise Profile Owner

Zasady haseł, aplikacji i bezpieczeństwa dla kontenera profilu służbowego



Android

Ograniczenia haseł i bezpieczeństwa dla urządzeń z Androidem



iOS

Zasady haseł, aplikacji, edukacji, mediów i filtra treści dla iOS



macOS

Ograniczenia haseł, aplikacji, edukacji i funkcji dla macOS



Windows

Ustawienia haseł, aplikacji, BitLockera i bezpieczeństwa dla Windows

Android Enterprise Device Owner

Zaktualizowano: 8 cze 2026

Hasło

Poziom wymaganego hasła

- Polityka określa poziom hasła na urządzeniu. Po zastosowaniu, użytkownik musi ustawić hasło urządzenia.
 - Poziom brak dopuszcza brak hasła na urządzeniu
 - Poziom niski dopuszcza wzór i niezłożone hasło numeryczne
 - Poziom średni dopuszcza hasło numeryczne z minimalnie 4 znakami złożonymi
 - Poziom wysoki wymaga złożonego hasła numerycznego z minimalnie 8 znakami lub alfanumerycznego z minimalnie 6 znakami
 - Niestandardowy - numeryczne, wymaga hasło numeryczne o minimalnej długości 4 znaków
 - Niestandardowy - numeryczne złożone, wymaga hasło numeryczne złożone o minimalnej długości 4 znaków
 - Niestandardowy - alfanumeryczne, wymaga hasła alfanumerycznego o minimalnej długości 4 znaków z możliwością określenia wymaganej ilości znaków numerycznych, małych, dużych oraz specjalnych

Minimalna długość hasła

- Polityka określa minimalną długość hasła zastosowanego na urządzeniu.

Wymagana ilość znaków numerycznych

- Polityka określa ile znaków numerycznych musi pojawić się w hasle urządzenia.

Wymagana ilość małych znaków

- Polityka określa ile małych znaków a-z musi pojawić się w hasle urządzenia.

Wymagana ilość dużych znaków

- Polityka określa ile dużych znaków A-Z musi pojawić się w hasle urządzenia.

Wymagana ilość znaków specjalnych

- Polityka określa ile znaków specjalnych !@#\$%^&*()_+:"'{}| musi pojawić się w hasle urządzenia.

Ilość prób odblokowania

- Polityka określa liczbę błędnych prób wprowadzenia hasła, po których nastąpi wyczyszczenie danych urządzenia. Polityka nie wspiera Direct Boot, jeśli zabronione jest przywracanie urządzenia do ustawień fabrycznych.

Ilość zapamiętanych haseł

- Polityka określa jaka ilość haseł ma zostać zachowana jako niemożliwa do ustawienia przy jego zmianie. Polityka nie obowiązuje, jeśli na urządzeniu ustawionym typem hasła jest wzór.

Ważność hasła

- Polityka określa jak długo hasło może być używane. Określa czas, po którym użytkownik musi zmienić hasło na urządzeniu.

Pozwalaj odblokować urządzenie za pomocą odcisku palca

- Polityka określa czy użytkownik może użyć odcisku palca do odblokowania urządzenia. Producent może wymagać nałożenia określonego typu hasła gdy ustawienie jest włączone.

Pozwalaj na skaner tęczówki

- Funkcja umożliwia użytkownikowi konfigurację skanera tęczówki i wykorzystanie tej funkcji do odblokowywania urządzenia. Ta polityka ma zastosowanie tylko do urządzeń posiadających system Android 9.0 lub nowszy. Producent może wymagać nałożenia określonego typu hasła gdy ustawienie jest włączone.

Pozwalaj na rozpoznawanie twarzy

- Funkcja umożliwia użytkownikowi konfigurację rozpoznawania twarzy i wykorzystanie tej funkcji do odblokowywania urządzenia. Ta polityka ma zastosowanie tylko do urządzeń posiadających system Android 9.0 lub nowszy. Producent może wymagać nałożenia określonego typu hasła gdy ustawienie jest włączone.

Wymagaj wiadomości na zablokowanym ekranie

- Polityka określa czy na zablokowanym ekranie urządzenia ma być widoczny zdefiniowany komunikat.

Wiadomość na ekranie blokady

- W okienku można zdefiniować wiadomość, która jest wysyłana do urządzenia i wyświetlana na zablokowanym ekranie urządzenia. W okienku działają zmienne globalne. Czyli, jeżeli ustawimy

np. {UserDisplayName}, to do urządzenia objętego tą polityką zostanie wysłana wartość pasująca pod zmienną globalną dla danego użytkownika.

Wymagaj blokady urządzenia przy błędnym hasle

- Polityka pozwala wprowadzić blokadę urządzenia po określonej ilości nieudanych prób wpisania hasła przez użytkownika. Polityka działa równocześnie z polityką "Ilość prób odblokowania".

Ilość prób odblokowania

- Polityka określa ilość błędnych prób wprowadzenia hasła, jakie użytkownik może wykonać przed zablokowaniem urządzenia.

Wiadomość na zablokowanym urządzeniu

- Wprowadź wiadomość, która ma się znaleźć na zablokowanym urządzeniu.

Numer telefonu

- Wprowadź numer telefonu, na który użytkownik może wykonać połączenie przy zablokowanym urządzeniu.

Aplikacje

Pozwalaj odinstalowywać aplikacje

- Polityka określa czy użytkownik może odinstalować aplikacje zainstalowane na urządzeniu.

Pozwalaj na dostęp do publicznych aplikacji w sklepie Google Play

- Polityka określa czy użytkownik ma dostęp do publicznych aplikacji w sklepie Google Play.

Określ sposób nadawania uprawnień do uruchomienia aplikacji

- Polityka określa sposób w jaki zostają nadane uprawnienia do uruchamiania aplikacji na urządzeniu. Polityka określa czy uprawnienia aplikacji przydzielają się automatycznie, zostają odrzucone automatycznie lub decyzję podejmuje użytkownik.

Aktualizacje aplikacji służbowych

- Polityka pozwala zdefiniować sposób aktualizacji aplikacji biznesowych.

Pozwalaj instalować aplikacje w połączeniach taryfowych

- Polityka określa czy na urządzeniu można instalować aplikacje w połączeniach taryfowych. Jeśli w Twojej sieci obowiązuje limit danych, możesz określić czy urządzenie będzie instalować aplikacje.

Wymuś użycie Play Protect

- Polityka wymusza wykorzystanie Play Protect do weryfikacji bezpieczeństwa nieznanymi aplikacjami.

Zarządzaj aktualizacjami aplikacji służbowych

- Polityka pozwala określić godziny aktualizacji aplikacji służbowych na urządzeniu. Funkcja nie ma zastosowania, gdy tryb automatycznej aktualizacji aplikacji ustawiono na wysoki priorytet.

Funkcjonalność

Pozwalaj używać Bluetooth

- Polityka określa czy można korzystać z bluetooth
 - Pozwalaj na udostępnianie przez Bluetooth
 - Polityka określa czy użytkownik może udostępniać dane poprzez Bluetooth.

Pozwalaj używać NFC

- Polityka określa czy można korzystać z NFC. Funkcja dostępna od Androida 15.

Pozwalaj na korzystanie z aparatu

- Polityka pozwala na wykorzystanie aparatu. Jeśli odznaczona, aparat nie będzie działał w żadnej aplikacji, w tym aplikacji Proget.

Pozwalaj używać mikrofonu

- Polityka pozwala na wykorzystanie mikrofonu. Jeśli odznaczona, mikrofon nie będzie działał w żadnej aplikacji, w tym aplikacji Proget.

Pozwalaj na konfigurację sieci komórkowej

- Polityka określa czy użytkownik może zmieniać ustawienia sieci komórkowej takich jak punkty dostępu, tryb pracy, operatorzy sieci.
 - Pozwalaj używać danych komórkowych podczas roamingu
 - Polityka określa czy użytkownik może wykorzystywać dane komórkowe kiedy urządzenie znajduje się w roamingu. Jeżeli polityka jest wyłączona, użytkownik nie może korzystać z Internetu kiedy urządzenie jest w roamingu.

Pozwalaj na konfigurację tetheringu oraz mobilnego punktu dostępu

- Polityka określa czy użytkownik może konfigurować tethering oraz mobilny punkt dostępu.

Pozwalaj edytować konfiguracje Wi-Fi

- Polityka określa czy użytkownik może dodać nowe połączenia Wi-Fi. Jeżeli polityka jest wyłączona, zostaje zablokowana możliwość konfigurowania nowych połączeń. Połączenia dodane przed zastosowaniem polityki będą nadal aktywne, ale bez możliwości edycji.

Określ ustawienia konfiguracji podtrzymania Wi-Fi po uśpieniu

- Polityka określa ustawienia podtrzymania połączenia z siecią Wi-Fi w momencie uśpienia urządzenia.

Pozwalaj usuwać dodane sieci Wi-Fi

- Polityka określa czy użytkownik może usuwać sieci Wi-Fi dodane przez administratora za pomocą profilu Wi-Fi.

Pozwalaj na tryb samolotowy

- Polityka pozwala na włączenie trybu samolotowego na urządzeniu. Funkcja dostępna od Android 9.

Pozwalaj konfigurować profil VPN

- Polityka określa czy użytkownik może samodzielnie konfigurować profil VPN oraz dokonywać zmiany ustawień dodanych połączeń VPN. Połączenia skonfigurowane przed zastosowaniem polityki będą nadal aktywne.

Pozwalaj na połączenia wychodzące

- Polityka określa czy użytkownik może wykonywać połączenia wychodzące.

Pozwalaj używać wiadomości SMS

- Polityka określa czy użytkownik może wysyłać i odbierać wiadomości SMS.

Pozwalaj na transfer plików przy użyciu połączenia USB

- Polityka określa czy użytkownik może przysyłać dane z urządzenia i na urządzenie przy użyciu połączenia USB.
 - Pozwalaj używać USB OTG
 - Polityka określa czy użytkownik może używać zewnętrznych pamięci masowych takich jak karta pamięci SD lub pendrive z wykorzystaniem złącza USB OTG.

Ustaw date i godzinę automatycznie

- Polityka określa czy użytkownik może zmieniać ustawienia daty i godziny. Jeżeli polityka jest włączona, użytkownik nie może ręcznie zmienić godziny i daty na urządzeniu.

Ustaw strefę czasową automatycznie

- Polityka określa czy urządzenie ma zmieniać automatycznie strefę czasową. Jeżeli polityka jest włączona, użytkownik nie będzie mógł zmienić strefy czasowej na urządzeniu.

Dozwolone metody wprowadzania danych

- Polityka określa czy użytkownik może używać jakichkolwiek metod wprowadzania danych (np. klawiatury), tylko metod dostarczanych przez urządzenie lub metod dostarczanych przez urządzenie i dodatkowych, które zostały określone.
 - Dozwolona aplikacja
 - Podaj package ID dozwolonej aplikacji np. com.android.example

Dozwolone serwisy dostępności

- Polityka określa serwisy dostępności, do których dostęp ma użytkownik. Domyślnie użytkownik może używać wszystkich serwisów dostępności. Systemem dostępności może być np. asystent głosowy.
 - Dozwolona aplikacja
 - Podaj package ID dozwolonej aplikacji np. com.android.example

Domyślny program uruchamiający

- Polityka określa identyfikator programu uruchamiającego, który musi być używany na urządzeniu. Żeby polityka mogła być zastosowana na urządzeniu, należy w pierwszej kolejności zainstalować aplikację programu uruchamiającego na urządzeniu.

Ogranicz użycie danych mobilnych przez aplikacje

- Podaj package ID aplikacji, które nie będą mogły korzystać z internetu za pośrednictwem danych mobilnych. Funkcja dostępna od Android 9.

Wymuś Always on VPN

- Polityka wymusza ciągłe podtrzymywanie połączenia przez wskazaną aplikację VPN.
 - Dodaj aplikację VPN
 - Zablokuj dostęp do internetu, gdy VPN nie jest połączony
 - Polityka wyłącza dostęp do internetu, jeśli połączenie VPN z wybranymi aplikacjami nie jest zestawione. Funkcja dostępna od Android 10.
 - Dodaj wyjątki

- Po dodaniu aplikacji do wyjątków, będą one mogły łączyć się z internetem pomimo ustawionej blokady. Funkcja dostępna od Android 10.

Pozwalaj na zmianę tapety ekranu

- Polityka określa czy użytkownik może zmieniać tapetę ekranu

Pozwalaj na usługi kopii zapasowej

- Polityka określa czy użytkownik może korzystać z usług kopii zapasowej

Ukryj ikonę Proget

- Jeśli zaznaczone, ikona aplikacji Proget na urządzeniu będzie ukryta

Zapytaj o dostęp do danych użycia urządzenia

- Jeśli zaznaczone, użytkownik zostanie poproszony o przydzielenie dostępu do danych użycia na urządzeniu

Ukryj notyfikację Proget

- Jeśli zaznaczone, notyfikacja Proget na urządzeniu będzie ukryta

Domyślna notyfikacja dla zarządzanego urządzenia

- Notyfikacja zostanie wyświetlona na urządzeniu które jest zarządzane przez aplikację Proget

Bezpieczeństwo

Zarządzaj kontami na urządzeniu

- Polityka określa konta, z których może korzystać użytkownik. Domyślnie użytkownik może korzystać ze wszystkich kont za wyjątkiem Google.

Pozwalaj wykonywać zrzuty ekranu

- Polityka określa czy użytkownik może wykonywać zrzuty ekranu.

Pozwalaj włączyć opcje programistyczne

- Polityka określa czy użytkownik może włączyć opcje programistyczne. Jeżeli polityka jest wyłączona, opcje programistyczne powracają do ustawień domyślnych.

Pozwalaj uruchomić tryb awaryjny na urządzeniu

- Polityka określa czy użytkownik może uruchomić tryb awaryjny na urządzeniu. W trybie awaryjnym urządzenie uruchamia się bez działania aplikacji trzecich.

Pozwalaj przywracać urządzenie do ustawień fabrycznych

- Polityka określa czy użytkownik może przywracać urządzenie do ustawień fabrycznych. Przywracanie do ustawień fabrycznych spowoduje usunięcie agenta MDM i utratę kontroli na urządzeniem.

Użyj Factory Reset Protection Uzyskaj Google ID

- Polityka wymusza wykorzystanie Factory Reset Protection. Jeżeli urządzenie zostanie przywrócone do ustawień fabrycznych, będzie wymagane podanie danych konta o Google ID podanym poniżej.

Pozwalaj użytkownikowi na dezaktywowanie agenta MDM

- Polityka określa czy użytkownik może dezaktywować urządzenie z poziomu agenta MDM.

Pozwalaj na czyszczenie danych aplikacji

Przestarzała

- Polityka pozwala na wyczyszczenie danych aplikacji Proget. Wyczyszczenie danych spowoduje odłączenie urządzenia od systemu.

Pozwalaj instalować aplikacje nie będące aplikacjami ze sklepu Google Play

- Polityka określa czy użytkownik może instalować aplikacje nie będące aplikacjami ze sklepu Google Play przy wykorzystaniu mechanizmu ACTION_INSTALL_PACKAGE.

Wymagaj rejestracji urządzenia w Microsoft Entra ID

- Polityka wymusza rejestrację użytkownika w Microsoft Entra ID. Jeżeli polityka zostanie włączona, urządzenie otrzyma polecenie logowania do konta Microsoft w celu jego rejestracji
 - Automatycznie ustaw login użytkownika
 - Ustawienie tego pola automatycznie wstawi określony login użytkownika podczas logowania do konta Microsoft.

Pozwalaj używać dwóch kart SIM jednocześnie

- Polityka określa czy użytkownik może korzystać z dwóch kart SIM jednocześnie jeżeli urządzenie obsługuje dwa wejścia na kartę SIM. Jeżeli polityka jest wyłączona, urządzenie zostanie zablokowane do momentu wyjęcia drugiej karty SIM.

Zablokuj kartę SIM kodem PIN dla slotu 1 (tylko Samsung)

- Polityka określa czy urządzenie ma zapisać stały kod PIN do odblokowania karty SIM. Włączenie stałego kodu PIN zablokuje użycie firmowej karty SIM na innym urządzeniu. Za każdym razem,

gdy urządzenie firmowe jest włączone, automatycznie odblokowuje kartę SIM, używając ustawionego kodu PIN. Jeśli jednak karta SIM zostanie przeniesiona na inne urządzenie, pozostanie zablokowana, ponieważ kod PIN nie jest znany użytkownikowi. Polityka ma zastosowanie dla slotu 1.

Zablokuj kartę SIM kodem PIN dla slotu 2 (tylko Samsung, jeżeli dostępny)

- Polityka określa czy urządzenie ma zapisać stały kod PIN do odblokowania karty SIM. Włączenie stałego kodu PIN zablokuje użycie firmowej karty SIM na innym urządzeniu. Za każdym razem, gdy urządzenie firmowe jest włączone, automatycznie odblokowuje kartę SIM, używając ustawionego kodu PIN. Jeśli jednak karta SIM zostanie przeniesiona na inne urządzenie, pozostanie zablokowana, ponieważ kod PIN nie jest znany użytkownikowi. Polityka ma zastosowanie dla slotu 2 (jeżeli dostępny).

Wymuś cykliczne pobieranie danych z serwera

- Polityka określa czy urządzenie ma pozyskiwać dane z serwera MDM co określony interwał czasowy. Włączenie polityki wymusza kontakt urządzenia z serwerem. Data ostatniego połączenia zostanie każdorazowo zapisana na serwerze.

Wymuś cykliczne przesyłanie danych na serwer

- Polityka określa czy urządzenie ma przysyłać dane do serwera MDM co określony interwał czasowy. Włączenie polityki wymusza kontakt urządzenia z serwerem. Data ostatniego połączenia zostanie każdorazowo zapisana na serwerze.

Maksymalny czas do blokady

- Polityka określa maksymalny czas aktywności użytkownika do zablokowania urządzenia. Ogranicza długość, którą użytkownik może ustawić w ustawieniach urządzenia.

Działanie po przekroczeniu czasu nieaktywności

- Polityka określa czy powinna zostać podjęta zdefiniowana akcja (Wyczyść dane urządzenia, Wyczyść dane służbowe lub Zablokuj urządzenie) po określonym czasie nieaktywności. Akcja zostanie podjęta automatycznie jeżeli ostatni kontakt urządzenia z serwerem przekroczy zdefiniowany czas nieaktywności.
 - Czas nieaktywności (w dniach)
 - Akcja
 - Wiadomość na zablokowanym urządzeniu
 - Wprowadź wiadomość, która ma się znaleźć na zablokowanym urządzeniu

- Numer telefonu
 - Wprowadź numer telefonu, na który użytkownik może wykonać połączenie przy zablokowanym urządzeniu.

Pozwalaj używać Smart Lock

- Polityka określa możliwość korzystania z funkcji Smart Lock na urządzeniu.
 - Bluetooth
 - Polityka pozwala na automatyczne odblokowanie telefonu, gdy jest połączony przez Bluetooth z zaufanym urządzeniem, takim jak zegarek czy samochodowy zestaw głośnomówiący.
 - NFC
 - Polityka pozwala na automatyczne odblokowanie telefonu za pomocą zaufanego tagu NFC.
 - Zaufane miejsce
 - Polityka pozwala konfigurować Zaufaną lokalizację. Urządzenie pozostaje automatycznie odblokowane w promieniu do 80 metrów od Zaufanego miejsca.
 - Face
 - Urządzenie automatycznie się odblokowuje, gdy rozpozna Twoją twarz. Jeśli skonfigurujesz zaufaną twarz, po każdym uruchomieniu urządzenie będzie jej szukać i odblokuje się, gdy ją rozpozna.
 - On-body
 - Polityka pozwala pozostawiać urządzenie odblokowane, gdy urządzenie jest przy użytkowniku (np. w ręce, kieszeni lub torbie). Urządzenie zablokuje się dopiero po odłożeniu urządzenia (np. na stół); blokada włączy się automatycznie w ciągu minuty.
 - Voice
 - Polityka pozwala na odblokowanie Asystenta Google po wypowiedzeniu na ekranie blokady słów "OK Google" i rozpoznaniu wcześniej zapisanego głosu. Można wydawać Google polecenia lub otwierać strony internetowe bez potrzeby ręcznego odblokowywania urządzenia.

Hasło serwisowe

Przestarzała

- Hasło serwisowe pozwala zdefiniować hasło do odblokowania zablokowanego urządzenia, tzw. lost mode. Hasło zdefiniowane w polityce działa równocześnie z hasłem znajdującym się na karcie urządzenia.

Powiadomienia na zablokowanym ekranie

- Polityka pozwala określić maksymalny poziom szczegółowości informacji w notyfikacjach na zablokowanym ekranie (użytkownik zawsze może zmniejszyć ten poziom manualnie).

Przechowywanie zdjęć z blokady urządzenia

- Polityka określa maksymalny czas przechowywania zdjęć na serwerze wykonanych podczas blokady urządzenia.

Zarządzanie aktualizacjami systemu operacyjnego

- Polityka pozwala określić sposób zarządzania aktualizacjami systemowymi na urządzeniu.

Zarządzanie Prywatnym DNS

- Polityka określa sposób konfiguracji Prywatnego DNS na urządzeniu. Opcja Oportunistyczny pozwala na automatyczne użycie prywatnego DNS, jeśli jest dostępny. Opcja Określony host wymaga podania konkretnego serwera DNS-over-TLS. Ta polityka ma zastosowanie tylko do urządzeń posiadających system Android 10 lub nowszy.

Lokalizacja

Zarządzaj trybami lokalizacji

- Polityka pozwala zdefiniować tryb, w jakim powinna być uruchamiana lokalizacja na urządzeniu. Funkcja dostępna na urządzeniach z Androidem niższym niż 9.

Zarządzaj stanem lokalizacji

- Polityka pozwala ustawić usługi lokalizacyjne na urządzeniu. Funkcja dostępna od Androida 11.

Android Enterprise Profile Owner

Zaktualizowano: 8 cze 2026

Hasło - Urządzenie

Poziom wymaganego hasła

- Polityka określa poziom hasła na urządzeniu. Po zastosowaniu, użytkownik musi ustawić hasło urządzenia.
 - Poziom brak dopuszcza brak hasła na urządzeniu
 - Poziom niski dopuszcza wzór i niezłożone hasło numeryczne
 - Poziom średni dopuszcza hasło numeryczne z minimalnie 4 znakami złożonymi
 - Poziom wysoki wymaga złożonego hasła numerycznego z minimalnie 8 znakami lub alfanumerycznego z minimalnie 6 znakami
 - Niestandardowy - numeryczne, wymaga hasło numeryczne o minimalnej długości 4 znaków
 - Niestandardowy - numeryczne złożone, wymaga hasło numeryczne złożone o minimalnej długości 4 znaków
 - Niestandardowy - alfanumeryczne, wymaga hasło alfanumeryczne o minimalnej długości 4 znaków z możliwością określenia wymaganej ilości znaków numerycznych, małych, dużych oraz specjalnych

Minimalna długość hasła

- Polityka określa minimalną długość hasła zastosowanego na urządzeniu.

Wymagana ilość znaków numerycznych

- Polityka określa ile znaków numerycznych musi pojawić się w hasle urządzenia.

Wymagana ilość małych znaków

- Polityka określa ile małych znaków a-z musi pojawić się w hasle urządzenia.

Wymagana ilość dużych znaków

- Polityka określa ile dużych znaków A-Z musi pojawić się w hasle urządzenia.

Wymagana ilość znaków specjalnych

- Polityka określa ile znaków specjalnych !@#\$%^&*()_+<>:"'{}|, musi pojawić się w hasle urządzenia.

Ilość prób odblokowania

- Polityka określa liczbę błędnych prób wprowadzenia hasła, po których następuje wyczyszczenie kontenera. W przypadku aktywacji COPE, dane urządzenia zostaną usunięte. Polityka nie wspiera Bezpośredniego Uruchamiania, jeśli przywracanie urządzenia do ustawień fabrycznych jest zabronione.

Ilość zapamiętanych haseł

- Polityka określa jaka ilość haseł ma zostać zachowana jako niemożliwa do ustawienia przy jego zmianie. Polityka nie obowiązuje, jeśli na urządzeniu ustawionym typem hasła jest wzór.

Ważność hasła

- Polityka określa jak długo hasło może być używane. Określa czas, po którym użytkownik musi zmienić hasło na urządzeniu.

Pozwalaj odblokować urządzenie za pomocą odcisku palca

- Polityka określa czy użytkownik może użyć odcisku palca do odblokowania urządzenia. Producent może wymagać nałożenia określonego typu hasła gdy ustawienie jest włączone.

Pozwalaj na skaner tęczówki

- Funkcja umożliwia użytkownikowi konfigurację skanera tęczówki i wykorzystanie tej funkcji do odblokowywania urządzenia. Ta polityka ma zastosowanie tylko do urządzeń posiadających system Android 9.0 lub nowszy. Producent może wymagać nałożenia określonego typu hasła gdy ustawienie jest włączone.

Pozwalaj na rozpoznawanie twarzy

- Funkcja umożliwia użytkownikowi konfigurację rozpoznawania twarzy i wykorzystanie tej funkcji do odblokowywania urządzenia. Ta polityka ma zastosowanie tylko do urządzeń posiadających system Android 9.0 lub nowszy. Producent może wymagać nałożenia określonego typu hasła gdy ustawienie jest włączone.

Wymagaj wiadomości na ekranie blokady (tylko COPE)

- Polityka określa czy na zablokowanym ekranie urządzenia ma być widoczny zdefiniowany komunikat.

Wiadomość na ekranie blokady (tylko COPE)

- W okienku można zdefiniować wiadomość, która jest wysyłana do urządzenia i wyświetlana na zablokowanym ekranie urządzenia. W okienku działają zmienne globalne. Czyli, jeżeli ustawimy np. {UserDisplayName} to do urządzenia objętego tą polityką, zostanie wysłana wartość pasująca pod zmienną globalną dla danego użytkownika.

Hasło - Kontener

Poziom wymaganego hasła

- Polityka określa poziom hasła na urządzeniu. Po zastosowaniu, użytkownik musi ustawić hasło urządzenia.
 - Poziom brak dopuszcza brak hasła na urządzeniu
 - Poziom niski dopuszcza wzór i niezłożone hasło numeryczne
 - Poziom średni dopuszcza hasło numeryczne z minimalnie 4 znakami złożonymi
 - Poziom wysoki wymaga złożonego hasła numerycznego z minimalnie 8 znakami lub alfanumerycznego z minimalnie 6 znakami
 - Niestandardowy - numeryczne, dopuszcza hasło numeryczne o minimalnej długości 4 znaków
 - Niestandardowy - numeryczne złożone, dopuszcza hasło numeryczne złożone o minimalnej długości 4 znaków
 - Niestandardowy - alfanumeryczne, wymaga hasła alfanumerycznego o minimalnej długości 4 znaków z możliwością określenia wymaganej ilości znaków numerycznych, znaków małych, znaków dużych oraz znaków specjalnych

Minimalna długość hasła

- Polityka określa minimalną długość hasła zastosowanego na urządzeniu.

Wymagana ilość znaków numerycznych

- Polityka określa ile znaków numerycznych musi pojawić się w hasle urządzenia.

Wymagana ilość małych znaków

- Polityka określa ile małych znaków a-z musi pojawić się w hasle urządzenia.

Wymagana ilość dużych znaków

- Polityka określa ile dużych znaków A-Z musi pojawić się w hasle urządzenia.

Wymagana ilość znaków specjalnych

- Polityka określa ile znaków specjalnych !@#\$%^&*()_+<>:"'{}|, musi pojawić się w hasle urządzenia.

Ilość prób odblokowania

- Polityka określa liczbę błędnych prób wprowadzenia hasła, po których następuje wyczyszczenie kontenera. Dla aktywacji COPE, dane urządzenia zostaną usunięte. Polityka nie wspiera Bezpośredniego Uruchamiania, jeśli przywracanie urządzenia do ustawień fabrycznych jest zabronione.

Ilość zapamiętanych haseł

- Polityka określa jaka ilość haseł ma zostać zachowana jako niemożliwa do ustawienia przy jego zmianie. Polityka nie obowiązuje, jeśli na urządzeniu ustawionym typem hasła jest wzór.

Ważność hasła

- Polityka określa jak długo hasło może być używane. Określa czas, po którym użytkownik musi zmienić hasło na urządzeniu.

Pozwalaj odblokować urządzenie za pomocą odcisku palca

- Polityka określa czy użytkownik może użyć odcisku palca do odblokowania urządzenia. Producent może wymagać nałożenia określonego typu hasła gdy ustawienie jest włączone.

Pozwalaj na skaner tęczówki

- Funkcja umożliwia użytkownikowi konfigurację skanera tęczówki i wykorzystanie tej funkcji do odblokowywania urządzenia. Ta polityka ma zastosowanie tylko do urządzeń posiadających system Android 9.0 lub nowszy. Producent może wymagać nałożenia określonego typu hasła gdy ustawienie jest włączone.

Pozwalaj na rozpoznawanie twarzy

- Funkcja umożliwia użytkownikowi konfigurację rozpoznawania twarzy i wykorzystanie tej funkcji do odblokowywania urządzenia. Ta polityka ma zastosowanie tylko do urządzeń posiadających system Android 9.0 lub nowszy. Producent może wymagać nałożenia określonego typu hasła gdy ustawienie jest włączone.

Aplikacje

Zezwalaj na odinstalowywanie aplikacji

- Polityka określa, czy użytkownik może odinstalować aplikacje zainstalowane w kontenerze.

Zezwalaj na dostęp do publicznych aplikacji w Sklepie Google Play

- Polityka określa, czy użytkownik ma dostęp do publicznych aplikacji w Sklepie Google Play.

Określ, jak przyznawać uprawnienia dla aplikacji

- Polityka określa sposób przyznawania uprawnień dla aplikacji. Polityka określa, czy uprawnienia aplikacji są przyznawane automatycznie, są automatycznie odrzucane, czy użytkownik może decydować. Dla urządzeń z Androidem 12 i nowszym, automatyczne uprawnienia związane z czujnikami (np. `permission.CAMERA`) nie działają.

Aktualizacje aplikacji biznesowych

- Polityka pozwala określić, jak powinny być aktualizowane aplikacje biznesowe.

Zezwalaj na instalowanie aplikacji w połączeniach z limitem danych

- Polityka określa, czy urządzenie może instalować aplikacje w połączeniach z limitem danych. Jeśli Twoja sieć ma limit danych, możesz określić, czy urządzenie będzie instalować aplikacje.

Wymuś korzystanie z Play Protect

- Polityka wymusza korzystanie z Play Protect do weryfikacji bezpieczeństwa nieznanymi aplikacjami.

Zawieś korzystanie z prywatnych aplikacji (tylko COPE)

- Polityka pozwala zawiesić korzystanie z prywatnych aplikacji. Gdy prywatne aplikacje są zawieszone, urządzenie może być używane tylko do dzwonienia.

Pozwalaj na udostępnianie danych z równoważnych aplikacji między przestrzeniami

- Polityka pozwala na udostępnianie danych z równoważnych aplikacji, znajdującymi się między przestrzenią prywatną i służbową. Funkcja dostępna od Android 11.
 - Dozwolona aplikacja
 - `policy.field.applications.allowed_cross_profile_apps_list.description`

Funkcjonalność

Dozwolone metody wprowadzania danych

- Polityka określa czy użytkownik może używać jakichkolwiek metod wprowadzania danych (np. klawiatury), tylko metod dostarczanych przez urządzenie lub metod dostarczanych przez urządzenie i dodatkowych, które zostały określone.
 - Dozwolona aplikacja
 - Podaj package ID dozwolonej aplikacji np. `com.android.example`

Pozwalaj używać aparatu

- Polityka pozwala na wykorzystanie aparatu. Jeśli odznaczona, aparat nie będzie działał w żadnej aplikacji, w tym aplikacji Proget.

Dozwolone serwisy dostępności

- Polityka określa serwisy dostępności, do których dostęp ma użytkownik. Domyślnie użytkownik może używać wszystkich serwisów dostępności. Systemem dostępności może być np. asystent głosowy.
 - Dozwolona aplikacja
 - Podaj package ID dozwolonej aplikacji np. com.android.example

Ogranicz użycie danych mobilnych przez aplikacje

- Podaj package ID aplikacji, które nie będą mogły korzystać z internetu za pośrednictwem danych mobilnych. Funkcja dostępna od Android 9.

Pozwalaj na tryb samolotowy (tylko COPE)

- Polityka pozwala na włączenie trybu samolotowego na urządzeniu.

Pozwalaj używać Bluetooth (tylko COPE)

- Polityka określa czy można korzystać z Bluetooth
 - Pozwalaj na udostępnianie przez Bluetooth (tylko COPE)
 - Polityka określa czy użytkownik może udostępniać dane poprzez Bluetooth.

Pozwalaj używać NFC (tylko COPE)

- Polityka określa czy można korzystać z NFC. Funkcja dostępna od Androida 15.

Pozwalaj używać aparatu (tylko COPE)

- Polityka pozwala na wykorzystanie aparatu. Jeśli odznaczona, aparat nie będzie działał w żadnej aplikacji, w tym aplikacji Proget.

Pozwalaj na konfiguracje nadawania komórkowego (tylko COPE)

- Polityka pozwala na konfiguracje nadawania komórkowego. Nadawanie komórkowe polega na rozsyłaniu informacji do użytkowników sieci znajdujących się w zasięgu jednej stacji bazowej BTS.

Pozwalaj na konfiguracje dat (tylko COPE)

- Polityka pozwala na konfiguracje daty, czasu i strefy czasowej w ustawieniach.

Pozwalaj na zmianę ustawień sieci komórkowej (tylko COPE)

- Polityka określa czy użytkownik może zmieniać ustawienia sieci komórkowej takich jak punkty dostępu, tryb pracy, operatorzy sieci.

Pozwalaj na konfiguracje prywatnego DNS (tylko COPE)

- Polityka pozwala na zmianę konfiguracji prywatnego DNS.

Pozwalaj na konfigurację tetheringu oraz mobilnego punktu dostępu (tylko COPE)

- Polityka określa czy użytkownik może konfigurować tethering oraz mobilny punkt dostępu.

Pozwalaj edytować konfiguracje Wi-Fi (tylko COPE)

- Polityka określa czy użytkownik może dodać nowe połączenia Wi-Fi. Jeżeli polityka jest wyłączona, zostaje zablokowana możliwość konfigurowania nowych połączeń. Połączenia dodane przed zastosowaniem polityki będą nadal aktywne, ale bez możliwości edycji.

Pozwalaj na przechwytywanie treści (tylko COPE)

- Polityka określa czy dozwolone jest przechwytywanie treści do późniejszego użycia przez AI.

Pozwalaj na sugerowane treści (tylko COPE)

- Polityka określa czy użytkownik może otrzymywać sugestie treści dopasowanych na podstawie przechwytywania treści.

Maksymalny czas wyłączenia profilu do pracy w dniach (tylko COPE)

- Polityka określa maksymalny czas, przez jaki profil do pracy może być wyłączony. Jeśli profil zostanie wyłączony na dłużej, aplikacje osobiste na urządzeniu zostaną zawieszone.
 - Czas wyłączenia (w dniach)

Pozwalaj na wszystkie metody wprowadzania danych (tylko COPE)

- Polityka pozwala na użycie wszystkich metod wprowadzania danych (np. klawiatura), po odznaczeniu dozwolone są tylko systemowe. Polityka ma zastosowanie do urządzeń z systemem Android 12 lub nowszym.

Wymuś Always on VPN

- Polityka wymusza ciągle podtrzymywanie połączenia przez wskazaną aplikację VPN.
 - Dodaj aplikację VPN

- Zablokuj dostęp do internetu, gdy VPN nie jest połączony
 - Polityka wyłącza dostęp do internetu, jeśli połączenie VPN z wybranymi aplikacjami nie jest zestawione. Funkcja dostępna od Android 10.
- Dodaj wyjątki
 - Po dodaniu aplikacji do wyjątków, będą one mogły łączyć się z internetem pomimo ustawionej blokady. Funkcja dostępna od Android 10.

Zapytaj o dostęp do danych użycia urządzenia

- Jeśli zaznaczone, użytkownik zostanie poproszony o przydzielenie dostępu do danych użycia na urządzeniu

Domyślna notyfikacja dla zarządzanego urządzenia

- Notyfikacja zostanie wyświetlona na urządzeniu które jest zarządzane przez aplikację Proget

Bezpieczeństwo

Zarządzaj kontami na urządzeniu

- Polityka określa konta, z których może korzystać użytkownik. Domyślnie użytkownik może korzystać ze wszystkich kont za wyjątkiem Google.

Pozwalaj wykonywać zrzuty ekranu

- Polityka określa czy użytkownik może wykonywać zrzuty ekranu. Ta polityka dotyczy tylko kontenera.

Pozwalaj na kopiowanie tekstów pomiędzy kontenerem i urządzeniem

- Polityka określa czy użytkownik może kopiować między przestrzeniami treść wygenerowaną w kontenerze lub urządzeniu.

Pozwalaj na wyszukiwanie kontaktów służbowych w przestrzeni prywatnej

- Polityka określa czy użytkownik może wyszukiwać kontakty służbowe w przestrzeni prywatnej.

Pozwalaj na identyfikowanie kontaktu służbowego dla połączeń przychodzących

- Polityka określa czy informacje o ID rozmówcy z przestrzeni służbowej będą wyświetlane w przestrzeni osobistej.

Pozwalaj użytkownikowi na dezaktywowanie agenta MDM

- Polityka określa czy użytkownik może dezaktywować urządzenie z poziomu agenta MDM.

Pozwalaj na czyszczenie danych aplikacji

Przestarzała

- Polityka pozwala na wyczyszczenie danych aplikacji Proget. Wyczyszczenie danych spowoduje odłączenie urządzenia od systemu.

Wymagaj rejestracji urządzenia w Microsoft Entra ID

- Polityka wymusza rejestrację użytkownika w Microsoft Entra ID. Jeżeli polityka zostanie włączona, urządzenie otrzyma polecenie logowania do konta Microsoft w celu jego rejestracji.
 - Automatycznie ustaw login użytkownika
 - Ustawienie tego pola automatycznie wstawi określony login użytkownika podczas logowania do konta Microsoft.

Wymuś cykliczne pobieranie danych z serwera

- Polityka określa czy urządzenie ma pozyskiwać dane z serwera MDM co określony interwał czasowy. Włączenie polityki wymusza kontakt urządzenia z serwerem. Data ostatniego połączenia zostanie każdorazowo zapisana na serwerze.

Wymuś cykliczne przesyłanie danych na serwer

- Polityka określa czy urządzenie ma przysyłać dane do serwera MDM co określony interwał czasowy. Włączenie polityki wymusza kontakt urządzenia z serwerem. Data ostatniego połączenia zostanie każdorazowo zapisana na serwerze.

Maksymalny czas do blokady

- Polityka określa maksymalny czas aktywności użytkownika do zablokowania urządzenia. Ogranicza długość, którą użytkownik może ustawić w ustawieniach urządzenia.
 - Czas do blokady (w minutach)

Działanie po przekroczeniu czasu nieaktywności

- Polityka określa czy powinna zostać podjęta zdefiniowana akcja (Wyczyść dane służbowe lub Wyczyść dane urządzenia dla COPE) po określonym czasie nieaktywności urządzenia. Akcja zostanie podjęta automatycznie jeżeli ostatni kontakt urządzenia z serwerem przekroczy zdefiniowany czas nieaktywności.
 - Czas nieaktywności (w dniach)
 - Akcja

Pozwalaj na udostępnianie kontaktów przez Bluetooth

- Polityka określa czy użytkownik może udostępniać kontakty z przestrzeni służbowej poprzez Bluetooth.

Pozwalaj na używanie Smart Lock

- Polityka definiuje możliwość wykorzystania funkcji Smart Lock na urządzeniach.
 - Bluetooth
 - Polityka pozwala na automatyczne odblokowanie telefonu, gdy jest połączony przez Bluetooth z zaufanym urządzeniem, takim jak zegarek czy samochodowy zestaw głośnomówiący.
 - NFC
 - Polityka pozwala na automatyczne odblokowanie telefonu za pomocą zaufanego tagu NFC.
 - Zaufane miejsce
 - Polityka pozwala konfigurować Zaufaną lokalizację. Urządzenie pozostaje automatycznie odblokowane w promieniu do 80 metrów od Zaufanego miejsca.
 - Face
 - Urządzenie automatycznie się odblokowuje, gdy rozpozna Twoją twarz. Jeśli skonfigurujesz zaufaną twarz, po każdym uruchomieniu urządzenie będzie jej szukać i odblokuje się, gdy ją rozpozna.
 - On-body
 - Polityka pozwala pozostawiać urządzenie odblokowane, gdy urządzenie jest przy użytkowniku (np. w ręce, kieszeni lub torbie). Urządzenie zablokuje się dopiero po odłożeniu urządzenia (np. na stół); blokada włączy się automatycznie w ciągu minuty.
 - Voice
 - Polityka pozwala na odblokowanie Asystenta Google po wypowiedzeniu na ekranie blokady słów "OK Google" i rozpoznaniu wcześniej zapisanego głosu. Można wydawać Google polecenia lub otwierać strony internetowe bez potrzeby ręcznego odblokowywania urządzenia.

Hasło serwisowe

Przestarzała

- Hasło serwisowe pozwala zdefiniować hasło do odblokowania zablokowanego urządzenia, tzw. lost mode. Hasło zdefiniowane w polityce działa równocześnie z hasłem znajdującym się na karcie urządzenia.

Pozwalaj instalować aplikacje nie będące aplikacjami ze sklepu Google Play

- Polityka określa czy użytkownik może instalować aplikacje nie będące aplikacjami ze sklepu Google Play. Polityka 'Nie pozwalaj' jest dostępna na urządzeniach z systemem Android 10 lub nowszym, dla urządzeń z Androidem starszym niż 10 polityka zadziała tak jak 'Pozwalaj tylko w przestrzeni prywatnej'.

Pozwalaj wykonywać zrzuty ekranu (tylko COPE)

- Polityka określa czy użytkownik może wykonywać zrzuty ekranu.

Użyj Factory Reset Protection (tylko COPE) Uzyskaj Google ID

- Polityka wymusza wykorzystanie Factory Reset Protection. Jeżeli urządzenie zostanie przywrócone do ustawień fabrycznych, będzie wymagane podanie danych konta o Google ID podanym poniżej.

Pozwalaj włączyć opcje programistyczne (tylko COPE)

- Polityka określa czy użytkownik może włączyć opcje programistyczne. Jeżeli polityka jest wyłączona, opcje programistyczne powracają do ustawień domyślnych.

Zarządzanie aktualizacjami systemu operacyjnego (tylko COPE)

- Polityka pozwala określić sposób zarządzania aktualizacjami systemowymi na urządzeniu.
 - Tryb
 - Określenie trybu aktualizacji.
 - Od
 - Określenie początku okresu aktualizacji.
 - Do
 - Określenie końca okresu aktualizacji.

Android

Zaktualizowano: 8 cze 2026

Hasło

Poziom wymaganego hasła

- Polityka określa poziom hasła na urządzeniu. Po zastosowaniu, użytkownik musi ustawić hasło urządzenia.
 - Poziom niski dopuszcza wzór i niezłożone hasło numeryczne
 - Poziom średni dopuszcza hasło numeryczne z minimalnie 4 znakami złożonymi
 - Poziom wysoki wymaga złożonego hasła numerycznego z minimalnie 8 znakami lub alfanumerycznego z minimalnie 6 znakami

Minimalna długość hasła

- Polityka określa minimalną długość hasła zastosowanego na urządzeniu.

Wymagana ilość znaków numerycznych

- Polityka określa ile znaków numerycznych musi pojawić się w hasle urządzenia.

Wymagana ilość małych znaków

- Polityka określa ile małych znaków a-z musi pojawić się w hasle urządzenia.

Wymagana ilość dużych znaków

- Polityka określa ile dużych znaków A-Z musi pojawić się w hasle urządzenia.

Wymagana ilość znaków specjalnych

- Polityka określa ile znaków specjalnych `!@#$%^&*()_+<>:"'{}|` musi pojawić się w hasle urządzenia.

Ilość prób odblokowania

- Polityka określa ile haseł wstecz powinno pamiętać urządzenie w trakcie wywoływania zmiany hasła.
- Polityka określa jaka ilość haseł ma zostać zachowana jako niemożliwa do ustawienia przy jego zmianie. Polityka nie obowiązuje, jeśli na urządzeniu ustawionym typem hasła jest wzór.

Ważność hasła

- Polityka określa jak długo hasło może być używane. Określa czas, po którym użytkownik musi zmienić hasło na urządzeniu.

Pozwalaj odblokować urządzenie za pomocą odcisku palca

- Polityka określa czy użytkownik może użyć odcisku palca do odblokowania urządzenia. Producent może wymagać nałożenia określonego typu hasła gdy ustawienie jest włączone.

Pozwalaj na skaner tęczówki

- Funkcja umożliwia użytkownikowi konfigurację skanera tęczówki i wykorzystanie tej funkcji do odblokowywania urządzenia. Ta polityka ma zastosowanie tylko do urządzeń posiadających system Android 9.0 lub nowszy. Producent może wymagać nałożenia określonego typu hasła gdy ustawienie jest włączone.

Pozwalaj na rozpoznawanie twarzy

- Funkcja umożliwia użytkownikowi konfigurację rozpoznawania twarzy i wykorzystanie tej funkcji do odblokowywania urządzenia. Ta polityka ma zastosowanie tylko do urządzeń posiadających system Android 9.0 lub nowszy. Producent może wymagać nałożenia określonego typu hasła gdy ustawienie jest włączone.

Bezpieczeństwo

Pozwalaj użytkownikowi na dezaktywowanie agenta MDM

- Polityka określa czy użytkownik może dezaktywować urządzenie z poziomu agenta MDM.

Pozwalaj na czyszczenie danych aplikacji

Przestarzała

- Polityka pozwala na wyczyszczenie danych aplikacji Proget. Wyczyszczenie danych spowoduje odłączenie urządzenia od systemu.

Działanie po przekroczeniu czasu nieaktywności

- Polityka określa czy powinna zostać podjęta zdefiniowana akcja (Wyczyść dane urządzenia lub Wyczyść dane służbowe) po określonym czasie nieaktywności urządzenia. Akcja zostanie podjęta automatycznie jeżeli ostatni kontakt urządzenia z serwerem przekroczy zdefiniowany czas nieaktywności.

Wymuś cykliczne pobieranie danych z serwera

- Polityka określa czy urządzenie ma pozyskiwać dane z serwera MDM co określony interwał czasowy. Włączenie polityki wymusza kontakt urządzenia z serwerem. Data ostatniego połączenia zostanie każdorazowo zapisana na serwerze.

Wymuś cykliczne przesyłanie danych na serwer

- Polityka określa czy urządzenie ma przysyłać dane do serwera MDM co określony interwał czasowy. Włączenie polityki wymusza kontakt urządzenia z serwerem. Data ostatniego połączenia zostanie każdorazowo zapisana na serwerze.

Wymagaj szyfrowania urządzenia

- Polityka wymusza szyfrowanie urządzenia, jeżeli jest obsługiwana przez urządzenie.

Pozwalaj na używanie Smart Lock

- Polityka definiuje możliwość wykorzystania funkcji Smart Lock na urządzeniach.
 - Bluetooth
 - Polityka pozwala na automatyczne odblokowanie telefonu, gdy jest połączony przez Bluetooth z zaufanym urządzeniem, takim jak zegarek czy samochodowy zestaw głośnomówiący.
 - NFC
 - Polityka pozwala na automatyczne odblokowanie telefonu za pomocą zaufanego tagu NFC.
 - Zaufane miejsce
 - Polityka pozwala konfigurować Zaufaną lokalizację. Urządzenie pozostaje automatycznie odblokowane w promieniu do 80 metrów od Zaufanego miejsca.
 - Face
 - Urządzenie automatycznie się odblokowuje, gdy rozpozna Twoją twarz. Jeśli skonfigurujesz zaufaną twarz, po każdym uruchomieniu urządzenie będzie jej szukać i odblokuje się, gdy ją rozpozna.
 - On-body
 - Polityka pozwala pozostawiać urządzenie odblokowane, gdy urządzenie jest przy użytkowniku (np. w ręce, kieszeni lub torbie). Urządzenie zablokuje się dopiero po odłożeniu urządzenia (np. na stół); blokada włączy się automatycznie w ciągu minuty.

- Voice
 - Polityka pozwala na odblokowanie Asystenta Google po wypowiedzeniu na ekranie blokady słów "OK Google" i rozpoznaniu wcześniej zapisanego głosu. Można wydawać Google polecenia lub otwierać strony internetowe bez potrzeby ręcznego odblokowywania urządzenia.

Hasło serwisowe

Przestarzała

- Hasło serwisowe pozwala zdefiniować hasło do odblokowania zablokowanego urządzenia, tzw. lost mode. Hasło zdefiniowane w polityce działa równocześnie z hasłem znajdującym się na karcie urządzenia.



Zaktualizowano: 13 sty 2025

Hasło

Wymaganie hasła

- Polityka określa wymagania dotyczące hasła na urządzeniu. Po zastosowaniu, użytkownik musi ustawić hasło urządzenia.

Długość hasła

- Polityka określa minimalną długość hasła zastosowanego na urządzeniu.

Wymagana ilość znaków specjalnych

- Polityka określa ile znaków specjalnych !@#\$%^&*()_+:"'{}|, musi pojawić się w hasle urządzenia.

Ilość prób odblokowania

- Polityka określa ile haseł wstecz powinno pamiętać urządzenie w trakcie wywoływania zmiany hasła.

Ilość zapamiętanych haseł

- Polityka określa ile haseł wstecz powinno pamiętać urządzenie w trakcie wywoływania zmiany hasła.

Ważność hasła (w dniach)

- Polityka określa jak długo hasło może być używane. Określa czas, po którym użytkownik musi zmienić hasło na urządzeniu. Wartość 0 oznacza, że hasło nie wygasa.

Okres karencji na blokadę urządzenia

- Polityka określa maksymalną długość czasu jaki ma użytkownik na ponowne odblokowanie urządzenia, bez potrzeby podawania hasła.

Pozwalaj używać Touch ID lub Face ID

- Polityka określa czy użytkownik może używać Touch ID lub Face ID do odblokowania urządzenia.

Pozwalaj na zmianę hasła (tryb nadzorowany)

- Polityka określa czy użytkownik może dodawać, zmieniać lub usuwać hasło urządzenia.

Pozwalaj modyfikować Touch ID lub Face ID (tryb nadzorowany)

- Polityka określa czy użytkownik może modyfikować Touch ID lub Face ID.

Maksymalny czas nieaktywności (w minutach)

- Polityka określa długość czasu nieaktywności użytkownika, po którym wygasza ekran i blokuje urządzenie aktualnym hasłem.

Pozwalaj na automatyczne odblokowywanie urządzenia

- Polityka określa czy funkcja automatycznego odblokowania urządzenia jest dostępna. Dostępne w iOS 14.5 i późniejszych.

Aplikacje

Pozwalaj na korzystanie ze sklepu iTunes

- Polityka określa czy można korzystać z sklepu iTunes.

Pozwalaj używać aplikacji News (tryb nadzorowany)

- Polityka określa czy użytkownik może korzystać z aplikacji News.

Pozwalaj używać podcastów (tryb nadzorowany)

- Polityka określa czy użytkownik może dodawać nowe podcasty.

Pozwalaj na App Clips (tryb nadzorowany)

- Jeśli odznaczone, uniemożliwia użytkownikowi dodawanie jakichkolwiek App Clips i usuwa wszystkie istniejące App Clips na urządzeniu. Wymaga nadzorowanego urządzenia. Dostępne w iOS 14.0 i nowszych.

Pozwalaj korzystać z Centrum Gier (tryb nadzorowany)

- Polityka określa czy Centrum Gier jest dostępne na urządzeniu. Jeżeli polityka jest wyłączona, ikona Centrum Gier jest usunięta z ekranu głównego i użytkownik nie może korzystać z Centrum Gier.

Pozwalaj na granie w trybie wieloosobowym (tryb nadzorowany)

- Polityka określa czy użytkownik może korzystać z gry w trybie wieloosobowym. Jeżeli polityka "Pozwalaj na dodawanie znajomych z Game Center" jest wyłączona, użytkownik może korzystać z gry w trybie wieloosobowym tylko z istniejącymi znajomymi. Jeżeli polityka jest wyłączona, użytkownik nie może korzystać z gry w trybie wieloosobowym oraz dodawać nowych znajomych w Centrum Gier.

Pozwalaj na dodawanie znajomych z Game Center (tryb nadzorowany)

- Jeśli odznaczone, zabrania dodawania znajomych do Game Center.

Pozwalaj korzystać z przeglądarki internetowej Safari (tryb nadzorowany)

- Jeśli odznaczone, wyłącza aplikację przeglądarki Safari, a jej ikona jest usuwana z ekranu głównego. To ustawienie uniemożliwia również użytkownikom otwieranie web clipów.
- Pozwalaj na autowypełnianie pól
 - Polityka określa czy przeglądarka może korzystać z opcji autowypełniania.
- Ostrzegaj przed oszustwem
 - Polityka określa czy przeglądarka internetowa Safari ma ostrzegać użytkownika jeżeli odwiedzi stronę internetową oznaczoną jako zagrożoną lub nieuczciwą.
- Pozwalaj na używanie JavaScript
 - Polityka określa czy Safari może korzystać z JavaScript. Wyłączenie tej funkcji zablokuje korzystanie ze sklepu z aplikacjami Proget.
- Pozwalaj na wyskakujące okienka
 - Polityka określa czy przeglądarka ma blokować wyskakujące okienka.
- Pozwalaj akceptować cookies
 - Polityka określa czy przeglądarka może korzystać z plików cookies.

Domyślne domeny

- Domeny email
 - Polityka określa domeny email, które zostaną uznane za domeny domyślne. Adresy email z pozostałych domen zostaną podkreślone jako domeny zewnętrzne w aplikacji Mail.
- Domeny internetowe
 - Polityka określa domeny, które zostaną uznane za domyślne. Oznacza to, że jeżeli za pomocą przeglądarki Safari zostanie pobrany dokument z domyślnej domeny, zostanie on uznany za element zarządzany. W zależności od polityki open-in, dokument będzie mógł być otwarty przez inne zarządzane lub niezarządzane aplikacje.

Nie pozwalaj na ręczne dodawanie haseł do pęku kluczy

- Polityka określa czy użytkownicy mogą ręcznie dodawać hasła do pęku kluczy. Jeśli odznaczona, użytkownicy mogą dodać witrynę, użytkownika i hasło z poziomu ustawień haseł.

Domeny

- Polityka określa czy użytkownicy mogą zapisywać hasła w Safari z adresów URL pasujących do wymienionych wzorców.

Pozwalaj instalować i aktualizować aplikacje (tryb nadzorowany)

- Jeśli odznaczone, wyłącza App Store, a jego ikona jest usuwana z ekranu głównego. Użytkownicy nie mogą instalować ani aktualizować swoich aplikacji.

Pozwalaj instalować i aktualizować aplikacje przez App Store (tryb nadzorowany)

- Polityka określa czy aplikacja App Store jest dostępna na urządzeniu. Jeżeli polityka jest wyłączona, nadal jest możliwość korzystania z aplikacji iTunes oraz aktualizowanie zainstalowanych aplikacji.

Pozwalaj na automatyczne pobieranie aplikacji (tryb nadzorowany)

- Polityka określa czy urządzenie może automatycznie pobierać aplikacje zakupione na innym urządzeniu. Polityka nie dotyczy aktualizacji istniejących aplikacji.

Pozwalaj korzystać z QuickPath (tryb nadzorowany)

- Jeśli odznaczone, wyłącza klawiaturę QuickPath.

Pozwalaj aplikacji Pliki na dostęp do dysków sieciowych (tryb nadzorowany)

- Jeśli odznaczone, uniemożliwia połączenie z dyskami sieciowymi w aplikacji Pliki.

Pozwalaj aplikacji Pliki na dostęp do innych urządzeń przez USB (tryb nadzorowany)

- Jeśli odznaczone, uniemożliwia połączenie z dowolnym podłączonym urządzeniem USB w aplikacji Pliki.

Pozwalaj korzystać z Find My Device (tryb nadzorowany)

- Jeśli odznaczone, wyłącza Znajdź moje urządzenie w aplikacji Znajdź moje.

Pozwalaj korzystać z Find My Friends (tryb nadzorowany)

- Jeśli odznaczone, wyłącza Znajdź moich znajomych w aplikacji Znajdź moje.

Pozwalaj na zapisywanie kontaktów w niezarządzalnych kontaktach

- Jeśli zaznaczone, zarządzane aplikacje mogą zapisywać kontakty na niezarządzanych kontaktach. Jeśli jest nadana polityka pozwalająca na otwieranie dokumentów z zarządzanych źródeł w niezarządzanych miejscach docelowych, to ograniczenie nie ma zastosowania.

Pozwalaj usuwać aplikacje systemowe (tryb nadzorowany)

- Jeśli odznaczone, wyłącza możliwość usuwania aplikacji systemowych z urządzenia.

Wymagaj zaufanych certyfikatów TLS dla AirPrint (tryb nadzorowany)

- Jeśli zaznaczone, wymaga zaufanych certyfikatów TLS do drukowania.

Wymuś automatyczną aktualizację aplikacji służbowych

- Polityka wymusza automatyczną aktualizację aplikacji służbowych na urządzeniach. Aplikacje zostaną zaktualizowane po wykryciu nowej wersji aplikacji dostępnej w App Store.

Edukacja

Pozwalaj na zdalny podgląd ekranu (tryb nadzorowany)

- Jeśli odznaczone, wyłącza zdalną obserwację ekranu przez aplikację Classroom. Jeśli opcja zezwolenia na zrzut ekranu jest odznaczone, aplikacja Classroom nie będzie mogła obserwować ekranów.

Wymagaj automatycznego dołączania do zajęć (tryb nadzorowany)

- Jeśli zaznaczone, automatycznie udziela uprawnień nauczycielowi bez monitorowania ucznia.

Wymagaj zgody na opuszczenie zajęć (tryb nadzorowany)

- Jeśli zaznaczone, uczeń zapisany na kurs niezarządzany przez Classroom musi prosić nauczyciela o zgodę na opuszczenie zajęć.

Pozwalaj blokować aplikacje i urządzenie (tryb nadzorowany)

- Jeśli zaznaczone, pozwala nauczycielowi zablokować aplikacje lub urządzenie bez pytania ucznia. Wymaga nadzorowanego urządzenia.

Pozwalaj na podgląd ekranu (tryb nadzorowany)

- Jeśli zaznaczone oraz "Pozwalaj na zdalny podgląd ekranu" jest również zaznaczone, uczeń zapisany na kurs zarządzany za pośrednictwem aplikacji Classroom automatycznie wyraża zgodę na prośby tego nauczyciela o obserwację ekranu ucznia bez monitorowania ucznia.

Funkcjonalność

Wymuś cykliczne połączenie urządzenia z serwerem

- Polityka określa czy urządzenie ma łączyć się do serwera MDM co określony interwał czasowy. Włączenie polityki wymusza kontakt urządzenia z serwerem. Data ostatniego połączenia zostanie każdorazowo zapisana na serwerze.

Pozwalaj używać aparatu

- Polityka pozwala na wykorzystanie aparatu. Jeśli odznaczona, aparat nie będzie działał w żadnej aplikacji, w tym aplikacji Proget.

Pozwalaj na korzystanie z FaceTime (tryb nadzorowany)

- Jeśli odznaczone, ukrywa aplikację FaceTime.

Pozwalaj wykonywać zrzuty ekranu oraz nagrywać ekran

- Polityka określa czy użytkownik może wykonywać zrzuty ekranu oraz nagrywać ekran.

Pozwalaj korzystać z AirDrop (tryb nadzorowany)

- Polityka określa czy użytkownik może korzystać z funkcji udostępniania AirDrop. Jeżeli polityka jest wyłączona, użytkownik nie może korzystać z funkcji AirDrop w żadnej z aplikacji oraz opcja AirDrop zostaje usunięta z Centrum Sterowania.

Pozwalaj korzystać z wiadomości iMessage (tryb nadzorowany)

- Polityka określa czy użytkownik może używać wiadomości iMessage.

Pozwalaj używać serwisu Muzyka Apple (tryb nadzorowany)

- Polityka określa czy użytkownik ma dostęp do serwisu Muzyka Apple. Jeżeli polityka jest wyłączona, aplikacja Muzyka powraca do klasycznego trybu.

Pozwalaj korzystać z radia (tryb nadzorowany)

- Polityka określa czy użytkownik może korzystać z serwisu iTunes radio.

Pozwalaj wykonywać połączenie głosowe, kiedy urządzenie jest zablokowane

- Polityka określa czy użytkownik może wykonywać połączenie głosowe, kiedy urządzenie jest zablokowane.

Pozwalaj korzystać z asystenta Siri

- Pozwalaj korzystać z asystenta Siri

Pozwalaj korzystać z asystenta Siri kiedy ekran urządzenia jest zablokowany

- Polityka określa, czy można korzystać z osobistego asystenta i nawigatora wiedzy podczas zablokowanego urządzenia.

Włącz filtr przekleństw w Siri (tryb nadzorowany)

- Polityka określa czy w asystencie Siri włączony jest filtr przekleństw.

Pokazuj treści wyszukiwania użytkownika w Siri (tryb nadzorowany)

- Polityka definiuje czy podczas korzystania z Siri widoczna jest treść wyszukiwania utworzona przez użytkownika.

Zabroń łączenia z serwerami Siri przy dyktowaniu

- Polityka wyłącza połączenia z serwerami asystenta Siri na potrzeby dyktowania. Dostępne w iOS 14.5 i nowszych.

Zabroń łączenia z serwerami Siri przy tłumaczeniu

- Polityka wyłącza połączenia z serwerami asystenta Siri na potrzeby tłumaczenia. Dostępne w iOS 15 i nowszych.

Pozwalaj korzystać ze sklepu iBooks (tryb nadzorowany)

- Polityka określa czy sklep iBooks jest dostępny na urządzeniu. Jeżeli polityka nie jest włączona, użytkownik nie posiada dostępu do sklepu iBooks

Pozwalaj usuwać aplikacje (tryb nadzorowany)

- Polityka określa czy użytkownik może usuwać aplikacje z urządzenia. Zastosowanie tej zasady do nienadzorowanego urządzenia może mieć nieoczekiwane rezultaty.

Pozwalaj na zakupy w aplikacjach

- Polityka określa, czy można wykonywać zakupy w aplikacjach.

Wymagaj hasła iTunes przy zakupach

- Polityka określa, czy jest wymagane hasło do iTunes przy zakupach w aplikacjach.

Pozwalaj korzystać z asystenta Siri

- Pozwalaj korzystać z asystenta Siri

Pozwalaj korzystać z asystenta Siri kiedy ekran urządzenia jest zablokowany

- Polityka określa, czy można korzystać z osobistego asystenta i nawigatora wiedzy podczas zablokowanego urządzenia.

Włącz filtr przekleństw w Siri (tryb nadzorowany)

- Polityka określa czy w asystencie Siri włączony jest filtr przekleństw.

Pokazuj treści wyszukiwania użytkownika w Siri (tryb nadzorowany)

- Polityka definiuje czy podczas korzystania z Siri widoczna jest treść wyszukiwania utworzona przez użytkownika.

Zabroń łączenia z serwerami Siri przy dyktowaniu

- Polityka wyłącza połączenia z serwerami asystenta Siri na potrzeby dyktowania. Dostępne w iOS 14.5 i nowszych.

Zabroń łączenia z serwerami Siri przy tłumaczeniu

- Polityka wyłącza połączenia z serwerami asystenta Siri na potrzeby tłumaczenia. Dostępne w iOS 15 i nowszych.

Pozwalaj korzystać ze sklepu iBooks (tryb nadzorowany)

- Polityka określa czy sklep iBooks jest dostępny na urządzeniu. Jeżeli polityka nie jest włączona, użytkownik nie posiada dostępu do sklepu iBooks

Pozwalaj usuwać aplikacje (tryb nadzorowany)

- Polityka określa czy użytkownik może usuwać aplikacje z urządzenia. Zastosowanie tej zasady do nienadzorowanego urządzenia może mieć nieoczekiwane rezultaty.

Pozwalaj na zakupy w aplikacjach

- Polityka określa, czy można wykonywać zakupy w aplikacjach.

Wymagaj hasła iTunes przy zakupach

- Polityka określa, czy jest wymagane hasło do iTunes przy zakupach w aplikacjach.

Pozwalaj na wykonywanie kopii zapasowej iCloud

- Polityka określa czy użytkownik ma możliwość wykonywania kopii zapasowej w iCloud.

Pozwalaj na synchronizację dokumentów z iCloud (tryb nadzorowany)

- Jeśli odznaczone, wyłącza synchronizację dokumentów i wartości klucza w iCloud

Pozwalaj na synchronizację pęku kluczy z iCloud

- Jeśli odznaczone, wyłącza synchronizację pęku kluczy z iCloud.

Pozwalaj zarządzanym aplikacjom na przechowywanie danych aplikacji w iCloud

- Polityka określa czy zarządzane aplikacje mogą przechowywać wewnętrzne dane aplikacji w iCloud.

Pozwalaj na kopię zapasową książek służbowych

- Polityka określa czy kopia zapasowa urządzenia może zawierać książki służbowe.

Pozwalaj synchronizować notatki i podkreślenia z książek służbowych

- Polityka określa czy urządzenie może synchronizować notatki i najważniejsze z książek służbowych.

Pozwalaj na udostępnianie zdjęć z iCloud

- Polityka określa czy użytkownik może włączyć udostępnianie zdjęć z iCloud. Jeżeli polityka jest wyłączona, użytkownik nie może udostępnić strumienia zdjęć dla innych ludzi. Jeżeli polityka zostanie wyłączona, zdjęcia i wideo mogą zostać utracone.

Pozwalaj korzystać z biblioteki zdjęć iCloud (tryb nadzorowany)

- Polityka określa czy użytkownik może zapisywać zdjęcia w bibliotece zdjęć iCloud.

Pozwalaj korzystać z iCloud Private Relay (tryb nadzorowany)

- Polityka określa czy usługa prywatności w internecie iCloud Private Relay jest dostępna. Dostępne w iOS 15 i nowszych.

Pozwalaj na ochronę prywatności w aplikacji Mail

- Jeśli zaznaczone, Twój adres IP jest ukryty przed nadawcami, a zdalna zawartość jest pobierana prywatnie w tle po otrzymaniu wiadomości (zamiast podczas jej przeglądania). Dostępne w iOS 15.2 i nowszych.

Pozwalaj używać NFC (tryb nadzorowany)

- Polityka określa czy można korzystać z NFC. Dostępne w iOS 14.2 i nowszych.

Pozwalaj na korzystanie ze strumienia zdjęć

- Polityka określa czy użytkownik może włączyć strumień zdjęć. Jeżeli polityka jest wyłączona, zdjęcia w strumieniu zdjęć będą usunięte z urządzenia, a zdjęcia z rolki aparatu nie będą dłużej dodawane do strumienia zdjęć.

Pozwalaj synchronizować dane w roamingu

- Polityka określa, czy urządzenie może automatycznie synchronizować dane w roamingu.

Wymuszaj szyfrowanie kopii zapasowej urządzenia

- Polityka określa czy zostaną wymuszone zaszyfrowane kopie zapasowe.

Pozwalaj na uruchamianie trybu odzyskiwania przez niesparowane urządzenia (tryb nadzorowany)

- Polityka umożliwia uruchamianie urządzeń do odzyskiwania przez niesparowane urządzenie. Wymaga urządzenia nadzorowanego. Dostępne w iOS 14.5 i nowszych.

Wymuś ograniczone śledzenie reklam

- Polityka określa czy aplikacje na urządzeniu mogą używać identyfikatorów reklamy, aby zapewnić ukierunkowane reklamy w aplikacjach.

Pozwalaj na spersonalizowane reklamy Apple

- Jeśli odznaczone, ogranicza spersonalizowane reklamy Apple. Dostępne w iOS 14 i nowszych.

Pozwalaj używać opcji Wymaż zawartość i ustawienia (tryb nadzorowany)

- Polityka określa czy użytkownik może używać opcji Wymaż zawartość i ustawienia w celu przywrócenia urządzenia do ustawień fabrycznych.

Pozwalaj użytkownikowi akceptować niezaufane certyfikaty TLS

- Polityka określa czy można akceptować niezaufane certyfikaty TLS.

Zezwalaj na automatyczne aktualizacje ustawień zaufania certyfikatów

- Polityka określa czy urządzenie umożliwia aktualizację zaufanych certyfikatów za pośrednictwem połączenia bezprzewodowego.

Pozwalaj na instalowanie dodatkowych profili konfiguracji (tryb nadzorowany)

- Polityka określa czy użytkownik może instalować dodatkowe profile konfiguracyjne na urządzeniu.

Pozwalaj modyfikować ustawienia kont (tryb nadzorowany)

- Polityka określa czy użytkownik może zmieniać ustawienia kont dodanych do urządzenia. Jeżeli polityka jest wyłączona, użytkownik nie może dodawać nowych kont oraz modyfikować ustawień obecnie używanych kont.

Pozwalaj zmieniać ustawienia Bluetooth (tryb nadzorowany)

- Polityka określa czy użytkownik może zmieniać ustawienia Bluetooth na urządzeniu.

Pozwalaj zmieniać ustawienia danych komórkowych w aplikacjach (tryb nadzorowany)

- Polityka określa czy użytkownik może zmieniać ustawienia użycia danych komórkowych dla aplikacji zainstalowanych na urządzeniu.

Pozwalaj zmieniać nazwę urządzenia (tryb nadzorowany)

- Polityka określa czy użytkownik może zmienić nazwy urządzenia.

Pozwalaj modyfikować ustawienia 'Znajdź moich znajomych' (tryb nadzorowany)

- Polityka określa czy użytkownik może zmieniać ustawienia 'Znajdź moich znajomych'. Polityka działa jeżeli na urządzeniu zainstalowana jest aplikacja Moi znajomi.

Pozwalaj zmieniać ustawienia powiadomień (tryb nadzorowany)

- Polityka określa czy użytkownik może zmieniać ustawienia dotyczące powiadomień na urządzeniu.

Pozwalaj na konfigurowanie restrykcji (tryb nadzorowany)

- Polityka określa czy użytkownik może skonfigurować własne restrykcje na urządzeniu, aby zapobiec dostępowi do aplikacji lub funkcjonalności urządzenia.

Pozwalaj na zmianę tapety (tryb nadzorowany)

- Polityka określa czy użytkownik może korzystać z funkcji przenoszenia aktywności użytkownika pomiędzy wieloma urządzeniami związanymi z użytkownikiem.

Pozwalaj na dołączenie tylko do sieci Wi-Fi określonych w Profilu Wi-Fi (tryb nadzorowany)

- Polityka określa czy urządzenie może podłączyć się tylko do sieci bezprzewodowej Wi-Fi zainstalowanej przez profil zarządzający. Dostępne w iOS 14.5 i nowszych.

Pozwalaj parować urządzenie z komputerem, który nie jest Konfiguratorem Apple (tryb nadzorowany)

- Polityka określa czy urządzenie może być sparowane z komputerem, który nie jest konfiguratorem Apple.

Włącz Activation Lock dla urządzeń z Apple Business Manager (tryb nadzorowany)

- Polityka wymusza włączenie Activation Lock dla urządzeń w trybie nadzorowanym z Apple Business Manager.

Pozwalaj na Activation Lock (tryb nadzorowany)

- Polityka pozwala na włączenie Activation Lock dla urządzeń w trybie nadzorowanym.

Pozwalaj otwierać dokumenty z zarządzanych aplikacji w aplikacjach niezarządzanych

- Polityka określa czy użytkownik może otwierać dokumenty i załączniki z aplikacji osobistych i kont w zarządzanych aplikacjach. Aplikacja Safari i AirDrop w dalszym ciągu będzie wyświetlać wszystkie aplikacje jako możliwe źródło, w którym użytkownik może otworzyć dokumenty niezależnie od ustawienia dla tej reguły lub reguły 'Pozwalaj otwierać dokumenty z zarządzanych aplikacji w aplikacjach niezarządzanych'.

Pozwalaj otwierać dokumenty z zarządzanych aplikacji w aplikacjach zarządzanych

- Polityka określa czy użytkownik może otwierać dokumenty i załączniki z zarządzanych aplikacji i kont w aplikacjach osobistych. Aplikacja Safari i AirDrop w dalszym ciągu będzie wyświetlać wszystkie aplikacje jako możliwe źródło, w którym użytkownik może otworzyć dokumenty niezależnie od ustawienia dla tej reguły lub reguły 'Pozwalaj otwierać dokumenty z niezarządzanych aplikacji w aplikacjach zarządzanych'.

Pozwalaj używać AirDrop jako źródło otwierania w aplikacjach zarządzanych

- Polityka określa czy AirDrop ma być widoczny jako źródło otwierania w aplikacjach zarządzanych.

Pozwalaj korzystać z funkcji Handoff

- Polityka określa czy użytkownik może korzystać z funkcji przenoszenia aktywności użytkownika pomiędzy wieloma urządzeniami związanymi z użytkownikiem.

Pozwalaj korzystać z wyszukiwania internetowego za pomocą funkcji Spotlight (tryb nadzorowany)

- Polityka określa czy użytkownik może używać Spotlight do wyszukiwania treści w Internecie podczas szukania treści na urządzeniu.

Pozwalaj wysyłać dane diagnostyczne do Apple

- Polityka określa czy można wysyłać dane diagnostyczne do Apple.

Pozwalaj zmieniać ustawienia diagnostyki (tryb nadzorowany)

- Polityka określa czy użytkownik może zmieniać ustawienia wysyłania danych diagnostycznych do Apple..

Włącz wymuszanie wykrywania nadgarstka przez zegarek Apple

- Polityka określa czy zegarek Apple Watch musi korzystać z funkcji wykrywania nadgarstka.

Pozwalaj parować urządzenie z zegarkiem Apple Watch (tryb nadzorowany)

- Polityka określa czy użytkownik może parować urządzenie z zegarkiem Apple Watch.

Wymagaj podania kodu dostępu podczas pierwszego parowania urządzenia przy korzystaniu z funkcji AirPlay

- Polityka określa czy hasło jest wymagane podczas pierwszego parowania urządzenia wykorzystującego AirPlay. Jeżeli polityka jest włączona, wszystkie urządzenia otrzymujące zapytanie dotyczące AirPlay, muszą użyć hasła parowania.

Pozwalaj korzystać z przewidywania pisowni (tryb nadzorowany)

- Polityka określa czy użytkownik może wykorzystywać przewidywanie tekstu.

Pozwalaj korzystać ze skrótów klawiszowych (tryb nadzorowany)

- Polityka określa czy użytkownik może wykorzystywać skróty klawiszowe na klawiaturze urządzenia.

Pozwalaj korzystać z automatycznej korekty pisowni (tryb nadzorowany)

- Polityka określa czy użytkownik może korzystać z autokorekty pisowni.

Pozwalaj używać sprawdzania pisowni (tryb nadzorowany)

- Polityka określa czy użytkownik może wykorzystywać sprawdzanie pisowni podczas pisania tekstu.

Pozwalaj używać funkcji Define (tryb nadzorowany)

- Polityka określa czy użytkownik może korzystać z funkcji Define, pozwalającej na wyszukiwanie definicji za pomocą podwójnego kliknięcia.

Pokazuj powiadomienia z aplikacji Wallet na zablokowanym ekranie

- Polityka określa czy powiadomienia z aplikacji Wallet mają być wyświetlane na zablokowanym ekranie urządzenia.

Pokazuj Centrum Sterowania na zablokowanym ekranie

- Polityka określa czy użytkownik ma dostęp do Centrum Sterowania na zablokowanym ekranie.

Pokazuj Centrum Powiadomień na zablokowanym ekranie

- Polityka określa czy użytkownik ma dostęp do widoku powiadomień w Centrum Powiadomień na zablokowanym ekranie.

Pokazuj widok dnia dzisiejszego na zablokowanym ekranie

- Polityka określa czy użytkownik ma dostęp do widoku dnia dzisiejszego w Centrum Powiadomień na zablokowanym ekranie.

Pozwalaj korzystać z AirPrint (tryb nadzorowany)

- Jeśli odznaczone, wyłącza AirPrint.

Pozwalaj przechowywać login i hasło do AirPrint (tryb nadzorowany)

- Jeśli odznaczone, wyłącza przechowywanie w pęku kluczy nazwy użytkownika i hasła dla AirPrint.

Pozwalaj na wykrywanie iBeacon (tryb nadzorowany)

- Jeśli odznaczone, wyłącza wykrywanie iBeacon drukarek AirPrint, co uniemożliwia fałszywym sygnalizatorom Bluetooth AirPrint wyłudzanie informacji o ruchu w sieci.

Pozwalaj na modyfikowanie planów danych sieci komórkowych (tryb nadzorowany)

- Jeśli odznaczone, użytkownicy nie mogą zmieniać żadnych ustawień związanych z planem komórkowym.

Pozwalaj na dyktowanie (tryb nadzorowany)

- Jeśli odznaczone, nie zezwala na wprowadzanie danych za pomocą dyktowania.

Pozwalaj na modyfikacje konfiguracji eSIM (tryb nadzorowany)

- Jeśli odznaczone, wyłącza modyfikacje ustawienia eSIM.

Pozwalaj na autouzupełnianie haseł (tryb nadzorowany)

- Jeśli odznaczone, wyłącza funkcję autouzupełniania haseł w systemie iOS (z pęku kluczy i menedżerami haseł innych firm) oraz użytkownik nie jest monitowany o możliwość użycia zapisanego hasła w przeglądarce Safari lub w aplikacjach.

Pozwalaj na żądanie hasła z pobliskich urządzeń (tryb nadzorowany)

- Jeśli odznaczone, wyłącza żądanie hasła z pobliskich urządzeń. Funkcja ograniczona do żądania hasła dostępu do Wi-Fi.

Pozwalaj na udostępnianie haseł przez AirDrop (tryb nadzorowany)

- Jeśli odznaczone, wyłącza udostępnianie haseł za pomocą funkcji Airdrop Passwords.

Pozwalaj na modyfikowanie ustawień hotspot (tryb nadzorowany)

- Jeśli odznaczone, wyłącza możliwość modyfikacji ustawień osobistego hotspotu.

Pozwalaj konfigurować nowe urządzenia (tryb nadzorowany)

- Jeśli odznaczone, wyłącza monit o konfigurację nowych urządzeń, które znajdują się w pobliżu. Wymaga nadzorowanego urządzenia.

Pozwalaj na dostęp do kontaktów z konta zarządzalnego aplikacjom niezarządzanym

- Jeśli niezaznaczone, niezarządzane aplikacje mogą odczytywać kontakty z zarządzanych kont kontaktów. Jeśli pozwalaj na otwieranie dokumentów ze źródeł zarządzanych w niezarządzanych miejscach docelowych jest zaznaczone, to ograniczenie nie ma zastosowania.

Pozwalaj podłączać urządzenia przez USB (tryb nadzorowany)

- Jeśli odznaczone, pozwala urządzeniu zawsze łączyć się z akcesoriami USB, gdy jest zablokowane.

Pozwalaj tworzyć VPN (tryb nadzorowany)

- Jeśli odznaczone, wyłącza możliwość tworzenia konfiguracji VPN.

Opóźnione aktualizacje systemu (tryb nadzorowany)

- Jeśli zaznaczone, opóźnia widoczność aktualizacji systemu dla użytkownika.

Opóźnij aktualizacje (tryb nadzorowany)

- Ustawia liczbę dni opóźnienia aktualizacji oprogramowania na urządzeniu. Po wprowadzeniu tego ograniczenia użytkownik nie widzi aktualizacji oprogramowania do określonej liczby dni po dacie wydania aktualizacji oprogramowania.

Wymagaj autoryzacji przed autouzupełnieniem (tryb nadzorowany)

- Jeśli zaznaczone, użytkownik musi się uwierzytelnić, zanim hasła lub informacje o karcie kredytowej będą mogły zostać automatycznie uzupełnione w Safari i aplikacjach. Jeśli to ograniczenie nie jest egzekwowane, użytkownik może przełączyć tę funkcję w Ustawieniach. Obsługiwane tylko na urządzeniach z Face ID lub Touch ID.

Wymagaj automatycznego ustawienia daty i czasu (tryb nadzorowany)

- Jeśli zaznaczone, aktywuje funkcję Ustaw automatycznie w opcji Data i godzina, która nie może być wyłączona przez użytkownika. Strefa czasowa urządzenia jest aktualizowana tylko wtedy, gdy urządzenie może określić swoją lokalizację za pomocą połączenia komórkowego lub Wi-Fi z włączonymi usługami lokalizacyjnymi.

Wymagaj korzystania z Wi-Fi (tryb nadzorowany)

- Jeśli zaznaczone, zapobiega wyłączaniu Wi-Fi w Ustawieniach lub Centrum sterowania, nawet przy wchodzeniu lub wychodzeniu z trybu samolotowego. Nie zapobiega to wyborowi, z której sieci Wi-Fi można korzystać.

Wymagaj Managed Pasteboard

- Pomaga kontrolować wklejanie treści z aplikacji, która korzysta z zarządzania Open In, przestrzegając obowiązujących ograniczeń Managed Open In. Aplikacje Apple współpracujące z zarządzanym wklejaniem obejmują Kalendarz, Pliki, Mail i Notatki. Aplikacje innych firm są kontrolowane w zależności od tego, czy są zarządzane. Gdy użytkownik próbuje wkleić zawartość tam, gdzie nie jest to dozwolone, pojawia się powiadomienie 'Wklejanie niedozwolone' wraz z nazwą organizacji (którą można zmienić w Ustawieniach). Aplikacje nie mogą również żądać elementów ze schowka, gdy to ograniczenie jest używane, a zawartość przekracza granicę zarządzaną.

Pozwalaj na instalację Rapid Security Response (tryb nadzorowany)

- Polityka określa czy użytkownik może instalować Rapid Security Response. Dostępne dla iOS 16 i nowszych.

Pozwalaj na usunięcie Rapid Security Response (tryb nadzorowany)

- Polityka określa czy użytkownik może usuwać Rapid Security Response. Dostępne dla iOS 16 i nowszych.

Media

Region oceny aplikacji

- Polityka określa jaki region ma być wykorzystywany do klasyfikacji treści.

Dozwolona ocena treści

Filmy

- Polityka określa maksymalną dozwoloną ocenę filmów, które użytkownik może pobrać z iTunes Store. Użycie tej reguły powoduje zablokowanie dostępu do nowych i istniejących filmów. Jeżeli wybrano opcję "Nie pozwalaj na filmy", wszystkie filmy zakupione w iTunes są ukryte, a użytkownik nie może przeglądać, kupować i pobierać filmów.

Programy telewizyjne

- Polityka określa maksymalną dozwoloną ocenę programów telewizyjnych, które użytkownik może pobrać z iTunes Store. Użycie tej reguły powoduje zablokowanie dostępu do nowych i istniejących programów telewizyjnych. Jeżeli wybrano opcję "Nie pozwalaj na programy telewizyjne", wszystkie programy telewizyjne zakupione w iTunes są ukryte, a użytkownik nie może przeglądać, kupować i pobierać programów telewizyjnych.

Aplikacje

- Polityka określa maksymalną dozwoloną ocenę aplikacji, które użytkownik może pobrać z iTunes Store. Użycie tej reguły powoduje zablokowanie dostępu do nowych i istniejących aplikacji. Ta polityka nie ma zastosowania dla aplikacji wbudowanych. Jeżeli wybrano opcję "Nie pozwalaj na aplikacje", wszystkie aplikacje zakupione w iTunes są ukryte, a użytkownik nie może przeglądać, kupować i pobierać aplikacji oraz ich aktualizacji.

Pozwalaj na odtwarzanie muzyki, podcastów oraz materiałów edukacyjnych iTunes, oznaczonych jako obraźliwe

- Polityka określa czy użytkownik może korzystać z materiałów uznanych jako obraźliwe pochodzących z muzyki, video oraz materiałów edukacyjnych. Jeżeli polityka jest wyłączona, materiały oznaczone jako obraźliwe zostaną ukryte, a użytkownik nie może wyświetlać i pobierać tych treści

Pozwalaj na treści seksualne w sklepie iBooks

- Polityka określa czy materiały o treści seksualnej zakupione w sklepie iBooks są dostępne na urządzeniu. Jeżeli polityka jest wyłączona, obraźliwe książki pobrane na urządzenie są ukryte a użytkownik nie może przeglądać i pobierać treści obraźliwych w sklepie iBooks.

Filtr treści WWW

Filtrowanie treści

- Zasady określa, czy możesz używać filtrów treści WWW, aby ograniczyć witryny internetowe, które użytkownik może przeglądać w Safari lub innych aplikacjach przeglądarkowych na urządzeniu z systemem iOS.

Włącz automatyczne filtrowanie (tryb nadzorowany)

- Ta opcja umożliwia automatyczne filtrowanie w celu identyfikacji i zablokowania nieodpowiedniej treści. Możesz także uwzględnić określone witryny internetowe, korzystając z następujących ustawień "Dozwolone adresy URL" i "Niedozwolone adresy URL"

Dozwolone adresy URL (tryb nadzorowany)

- Polityka określa, czy możesz dodać jeden lub więcej adresów URL, aby umożliwić dostęp do określonych witryn. Użytkownicy mogą przeglądać witryny na tej liście, niezależnie od tego, czy automatyczne filtrowanie blokuje dostęp.

Niedozwolone adresy URL (tryb nadzorowany)

- Polityka określa, czy możesz dodać jeden lub więcej adresów URL, aby odmówić dostępu do określonych witryn. Użytkownicy nie mogą wyświetlać witryn na tej liście, niezależnie od tego,

czy automatyczne filtrowanie umożliwia dostęp.

Określone adresy internetowe (tryb nadzorowany)

- Polityka określa, czy użytkownik ma dostęp tylko do określonych stron internetowych. Ponadto w Safari tworzona jest zakładka dla każdej dozwolonej witryny.

macOS

Zaktualizowano: 13 sty 2025

Hasło

Wymaganie hasła

- Polityka określa wymagania dotyczące hasła na urządzeniu. Po zastosowaniu, użytkownik musi ustawić hasło urządzenia.

Długość hasła

- Polityka określa minimalną długość hasła zastosowanego na urządzeniu.

Ilość prób odblokowania

- Polityka określa ilość błędnych prób wprowadzenia hasła, jakie użytkownik może wykonać przed zablokowaniem urządzenia.

Ilość zapamiętanych haseł

- Polityka określa ile haseł wstecz powinno pamiętać urządzenie w trakcie wywoływania zmiany hasła.

Ważność hasła (w dniach)

- Polityka określa jak długo hasło może być używane. Określa czas, po którym użytkownik musi zmienić hasło na urządzeniu. Wartość 0 oznacza, że hasło nie wygasa.

Okres karencji na blokadę urządzenia

- Polityka określa maksymalną długość czasu jaki ma użytkownik na ponowne odblokowanie urządzenia, bez potrzeby podawania hasła.

Pozwalaj odblokować urządzenie za pomocą odcisku palca

- Polityka określa czy użytkownik może użyć odcisku palca do odblokowania urządzenia. Jeżeli polityka jest wyłączona, użytkownik musi podać hasło, aby odblokować urządzenie.

Pozwalaj na zmianę hasła (tryb nadzorowany)

- Polityka określa czy użytkownik może dodawać, zmieniać lub usuwać hasło urządzenia.

Maksymalny czas nieaktywności (w minutach)

- Polityka określa długość czasu nieaktywności użytkownika, po którym wygasza ekran i blokuje urządzenie aktualnym hasłem.

Pozwalaj na automatyczne odblokowywanie urządzenia

- Polityka określa czy funkcja automatycznego odblokowania urządzenia jest dostępna.

Aplikacje

Pozwalaj na korzystanie ze sklepu App Store

- Polityka określa czy można korzystać ze sklepu App Store.

Pozwalaj korzystać z Centrum Gier (tryb nadzorowany)

- Polityka określa czy Centrum Gier jest dostępne na urządzeniu. Jeżeli polityka jest wyłączona, ikona Centrum Gier jest usunięta z ekranu głównego i użytkownik nie może korzystać z Centrum Gier.

Pozwalaj na granie w trybie wieloosobowym (tryb nadzorowany)

- Polityka określa czy użytkownik może korzystać z gry w trybie wieloosobowym. Jeżeli polityka "Pozwalaj na dodawanie znajomych z Game Center" jest wyłączona, użytkownik może korzystać z gry w trybie wieloosobowym tylko z istniejącymi znajomymi. Jeżeli polityka jest wyłączona, użytkownik nie może korzystać z gry w trybie wieloosobowym oraz dodawać nowych znajomych w Centrum Gier.

Pozwalaj na dodawanie znajomych z Game Center (tryb nadzorowany)

- Jeśli odznaczone, zabrania dodawania znajomych do Game Center.

Pozwalaj korzystać z iTunes Filesharing

- Jeśli odznaczone, wyłącza usługę iTunes Filesharing.

Pozwalaj na autowypełnianie pól

- Polityka określa czy przeglądarka może korzystać z opcji autowypełniania.

Domyślne domeny

Domeny email

- Polityka określa domeny email, które zostaną uznane za domeny domyślne. Adresy email z pozostałych domen zostaną podkreślone jako domeny zewnętrzne w aplikacji Mail.

Edukacja

Pozwalaj na zdalny podgląd ekranu (tryb nadzorowany)

- Jeśli odznaczone, wyłącza zdalną obserwację ekranu przez aplikację Classroom. Jeśli opcja zezwolenia na zrzut ekranu jest odznaczone, aplikacja Classroom nie będzie mogła obserwować ekranów.

Wymagaj automatycznego dołączania do zajęć (tryb nadzorowany)

- Jeśli zaznaczone, automatycznie udziela uprawnień nauczycielowi bez monitowania ucznia.

Wymagaj zgody na opuszczenie zajęć (tryb nadzorowany)

- Jeśli zaznaczone, uczeń zapisany na kurs niezarządzany przez Classroom musi prosić nauczyciela o zgodę na opuszczenie zajęć.

Pozwalaj blokować aplikacje i urządzenie (tryb nadzorowany)

- Jeśli zaznaczone, pozwala nauczycielowi zablokować aplikacje lub urządzenie bez pytania ucznia. Wymaga nadzorowanego urządzenia.

Pozwalaj na podgląd ekranu (tryb nadzorowany)

- Jeśli zaznaczone oraz "Pozwalaj na zdalny podgląd ekranu" jest również zaznaczone, uczeń zapisany na kurs zarządzany za pośrednictwem aplikacji Classroom automatycznie wyraża zgodę na prośby tego nauczyciela o obserwację ekranu ucznia bez monitowania ucznia. Wymaga nadzorowanego urządzenia.

Funkcjonalność

Pozwalaj używać aparatu

- Polityka pozwala na wykorzystanie aparatu. Jeśli odznaczona, aparat nie będzie działał w żadnej aplikacji.

Pozwalaj wykonywać zrzuty ekranu oraz nagrywać ekran

- Polityka określa czy użytkownik może wykonywać zrzuty ekranu oraz nagrywać ekran.

Pozwalaj korzystać z AirDrop (tryb nadzorowany)

- Polityka określa czy użytkownik może korzystać z funkcji udostępniania AirDrop. Jeżeli polityka jest wyłączona, użytkownik nie może korzystać z funkcji AirDrop w żadnej z aplikacji oraz opcja AirDrop zostaje usunięta z Centrum Sterowania.

Pozwalaj używać serwisu Muzyka Apple (tryb nadzorowany)

- Polityka określa czy użytkownik ma dostęp do serwisu Muzyka Apple. Jeżeli polityka jest wyłączona, aplikacja Muzyka powraca do klasycznego trybu.

Pozwalaj na synchronizację dokumentów z iCloud (tryb nadzorowany)

- Jeśli odznaczone, wyłącza synchronizację dokumentów i wartości klucza w iCloud.

Pozwalaj korzystać z Biurka i Dokumentów iCloud

- Jeśli odznaczone, wyłącza usługi chmurowe biurka i dokumentów.

Pozwalaj na synchronizację pęku kluczy z iCloud

- Jeśli odznaczone, wyłącza synchronizację pęku kluczy z iCloud.

Pozwalaj korzystać z biblioteki zdjęć iCloud (tryb nadzorowany)

- Polityka określa czy użytkownik może zapisywać zdjęcia w bibliotece zdjęć iCloud.

Pozwalaj korzystać z Kontakty iCloud

- Jeśli odznaczone, wyłącza usługi książki adresowej iCloud.

Pozwalaj korzystać z Zakładek iCloud

- Jeśli odznaczone, wyłącza synchronizację zakładek iCloud.

Pozwalaj korzystać z Kalendarza iCloud

- Jeśli odznaczone, wyłącza usługę Kalendarz iCloud.

Pozwalaj korzystać z iCloud Mail

- Jeśli odznaczone, wyłącza usługi poczty iCloud.

Pozwalaj korzystać z Notatek iCloud

- Jeśli odznaczone, wyłącza usługi Notatek iCloud.

Pozwalaj korzystać z Przypomnień iCloud

- Jeśli odznaczone, wyłącza usługę Przypomnienie iCloud.

Pozwalaj korzystać z iCloud Private Relay (tryb nadzorowany)

- Polityka określa czy usługa prywatności w internecie iCloud Private Relay jest dostępna.

Pozwalaj na zmianę tapety (tryb nadzorowany)

- Polityka określa czy użytkownik może zmieniać tapetę ekranu urządzenia.

Pozwalaj korzystać z funkcji Handoff

- Polityka określa czy użytkownik może korzystać z funkcji przenoszenia aktywności użytkownika pomiędzy wieloma urządzeniami związanymi z użytkownikiem.

Pozwalaj korzystać z wyszukiwania internetowego za pomocą funkcji Spotlight (tryb nadzorowany)

- Polityka określa czy użytkownik może korzystać z funkcji Spotlight do przeszukiwania Internetu podczas wyszukiwania treści na urządzeniu.

Pozwalaj wysyłać dane diagnostyczne do Apple

- Polityka określa czy można wysyłać dane diagnostyczne do Apple.

Pozwalaj na dyktowanie (tryb nadzorowany)

- Jeśli odznaczone, nie zezwala na wprowadzanie danych za pomocą dyktowania.

Pozwalaj na autouzupełnianie haseł (tryb nadzorowany)

- Jeśli odznaczone, wyłącza funkcję autouzupełniania haseł w systemie macOS (z pęku kluczy i menedżerami haseł innych firm), a użytkownik nie jest monitowany o możliwości użycia zapisanego hasła w przeglądarce Safari lub w aplikacjach.

Pozwalaj na żądanie hasła z pobliskich urządzeń (tryb nadzorowany)

- Jeśli odznaczone, wyłącza żądanie hasła z pobliskich urządzeń. Funkcja ograniczona do żądania hasła dostępu do Wi-Fi.

Pozwalaj na udostępnianie haseł przez AirDrop (tryb nadzorowany)

- Jeśli odznaczone, wyłącza udostępnianie haseł za pomocą funkcji Airdrop Passwords.

Włącz Activation Lock dla urządzeń z Apple Business Manager (tryb nadzorowany)

- Polityka wymusza włączenie Activation Lock dla urządzeń w trybie nadzorowanym z Apple Business Manager.

Pozwalaj na Activation Lock (tryb nadzorowany)

- Polityka pozwala na włączenie Activation Lock dla urządzeń w trybie nadzorowanym.

Wymuś opóźnienie aktualizacji oprogramowania aplikacyjnego (tryb nadzorowany)

- Jeśli zaznaczone, opóźnia widoczność aktualizacji oprogramowania innego niż systemowe.

Opóźnione aktualizacje systemu (tryb nadzorowany)

- Jeśli zaznaczone, opóźnia widoczność aktualizacji systemu przez użytkownika.

Opóźnij aktualizacje (tryb nadzorowany)

- Ustawia liczbę dni opóźnienia aktualizacji oprogramowania na urządzeniu. Po wprowadzeniu tego ograniczenia użytkownik nie zobaczy aktualizacji oprogramowania do określonej liczby dni po dacie wydania aktualizacji oprogramowania.

Windows

Zaktualizowano: 13 sty 2025

Hasło

Wymaganie hasła

- Polityka określa wymagania dotyczące hasła na urządzeniu. Po zastosowaniu, użytkownik musi ustawić hasło urządzenia.

Długość hasła

- Polityka określa minimalną długość hasła zastosowanego na urządzeniu.

Ważność hasła (w dniach)

- Polityka określa jak długo hasło może być używane i ustala czas, po którym użytkownik musi zmienić hasło na urządzeniu.

Maksymalny czas nieaktywności (w minutach)

- Polityka określa czas trwania nieaktywności użytkownika, po którym wygasa ekran i blokuje urządzenie aktualnym hasłem.

Ilość prób odblokowania

- Polityka określa ilość błędnych prób wprowadzenia hasła. Po przekroczeniu dopuszczalnej ilości, urządzenie uruchomi się ponownie

Aplikacje

Pozwalaj korzystać z Cortany

- Polityka określa korzystanie z asystenta głosowego Cortana na urządzeniu.

BitLocker

Włącz szyfrowanie urządzenia

- Włącz BitLocker - rozwiązanie pozwalające na kryptograficzną ochronę danych na dyskach, wbudowane w systemach operacyjnych Microsoftu.

Skonfiguruj metody szyfrowania dla dysków

- To ustawienie pozwala wybrać algorytm i siłę szyfrowania używaną przez funkcję BitLocker. To ustawienie jest stosowane po włączeniu funkcji BitLocker. Zmiana metody szyfrowania nie ma wpływu, jeśli dysk jest już zaszyfrowany lub szyfrowanie jest w toku.

Monituj o szyfrowanie urządzenia

- Włącz opcję "Monituj o szyfrowanie urządzenia", aby monitować użytkowników o zaszyfrowanie dysku systemowego.

Zezwalaj na standardowe szyfrowanie użytkownika

- Zasady pozwalają na egzekwowanie zasad szyfrowania urządzenia w scenariuszach, w których ustawienia są wypychane, gdy bieżącym zalogowanym użytkownikiem jest konto administratora Azure AD inne niż administrator / użytkownik standardowy. Ta polityka jest obsługiwana tylko na kontach Azure AD.

Skonfiguruj opcje odzyskiwania dla dysków wewnętrznych

- To ustawienie pozwala kontrolować sposób odzyskiwania dysków stałych chronionych funkcją BitLocker przy braku wymaganych poświadczeń. To ustawienie jest stosowane po włączeniu funkcji BitLocker.
 - Wymagaj szyfrowania dysków wewnętrznych
 - Jeśli włączysz to ustawienie, wszystkie dyski stałe, które nie są chronione funkcją BitLocker, zostaną zamontowane w trybie tylko do odczytu. Jeśli dysk jest chroniony przez BitLocker, będzie dostępny w trybie do odczytu i zapisu.
 - Skonfiguruj metody szyfrowania dla dysków wewnętrznych
 - W przypadku dysków wewnętrznych zalecamy użycie algorytmu XTS-AES.
 - Zapisz informacje o funkcji BitLocker na stałych dyskach danych w Azure AD DS.
 - Używaj agentów odzyskiwania danych dla dysków wewnętrznych
 - Agenci odzyskiwania danych mają uprawnienia do odszyfrowywania danych zaszyfrowanych przez innych użytkowników, ponieważ ich certyfikaty PKI zostały użyte do utworzenia ochrony klucza BitLocker. Mogą zatem użyć swoich danych uwierzytelniających do odblokowania dysków chronionych funkcją BitLocker.
 - Ukryj opcje odzyskiwania w kreatorze konfiguracji funkcji BitLocker
 - Zapobiegaj określaniu przez użytkownika opcji odzyskiwania po uruchomieniu funkcji BitLocker na dysku.

- Wyłącz BitLocker, aż informacje o odzyskiwaniu stałych dysków zostaną zapisane w Azure AD DS
 - Zapobiegij użytkownikowi włączania BitLocker, chyba że komputer jest podłączony do domeny i kopia zapasowa informacji o odzyskiwaniu danych BitLocker na platformie Azure AD DS udaje się.
- Wybierz informacje odzyskiwania, które mają być przechowywane w usłudze Azure AD DS.
- Wygeneruj klucz odzyskiwania
 - 256-bitowy klucz odzyskiwania jest generowany przez system i jest przechowywany na zewnętrznym napędzie USB.
- Wygeneruj hasło odzyskiwania
 - 48-cyfrowe hasło odzyskiwania jest generowane przez system i jest drukowane lub przechowywane na zewnętrznym napędzie USB.
- Wymagaj szyfrowania dysków wymiennych
 - Jeśli włączysz to ustawienie, wszystkie dyski wymienne, które nie są chronione funkcją BitLocker, zostaną zamontowane w trybie tylko do odczytu. Jeśli dysk jest chroniony przez BitLocker, będzie dostępny w trybie do odczytu i zapisu.
- Skonfiguruj metody szyfrowania dla dysków wymiennych
 - W przypadku dysków wymiennych należy użyć 128-bitowego AES-CBC lub 256-bitowego AES-CBC, jeśli dysk będzie używany w innych urządzeniach, na których nie jest uruchomiony system Windows 10 w wersji 1511.
- Skonfiguruj metody szyfrowania dla dysków systemowych
 - W przypadku dysków systemowych zalecamy użycie algorytmu XTS-AES.
- Minimalna długość kodu PIN funkcji BitLocker z TPM
 - To ustawienie pozwala skonfigurować minimalną długość kodu PIN dla autoryzacji z wykorzystaniem TPM. Początkowy kod PIN musi mieć minimalną długość 6 cyfr i może mieć maksymalną długość 20 cyfr.
- Skonfiguruj komunikat odzyskiwania
- Niestandardowy komunikat odzyskiwania i adres URL
- Skonfiguruj opcje odzyskiwania dla dysków systemowych
 - Skonfiguruj sposób odzyskiwania dysków systemowych chronionych funkcją BitLocker.

- Używaj agentów odzyskiwania danych z dysków systemowych
 - Agenci odzyskiwania danych mają uprawnienia do odszyfrowywania danych zaszyfrowanych przez innych użytkowników, ponieważ ich certyfikaty PKI zostały użyte do utworzenia ochrony klucza BitLocker. Mogą zatem użyć swoich danych uwierzytelniających do odblokowania dysków chronionych funkcją BitLocker.
- Ukryj opcje odzyskiwania w kreatorze konfiguracji funkcji BitLocker
 - Zapobiegaj określaniu przez użytkownika opcji odzyskiwania po uruchomieniu funkcji BitLocker na dysku.
- Wyłącz BitLocker, aż informacje o odzyskiwaniu dysku systemowego będą przechowywane w usłudze Azure AD DS
 - Zapobiegaj włączaniu funkcji BitLocker przez użytkownika, chyba że komputer jest podłączony do domeny i kopia zapasowa informacji o odzyskiwaniu danych Bitlocker na platformie Azure AD DS udaje się.
- Wybierz informacje odzyskiwania, które mają być przechowywane w usłudze Azure AD DS.
- Skonfiguruj sposób uwierzytelniania podczas uruchamiania komputera
 - To ustawienie pozwala skonfigurować, czy BitLocker ma wymagać dodatkowego uwierzytelniania przy każdym uruchomieniu komputera i czy używasz TPM (Trusted Platform Module).
- Włącz funkcję BitLocker bez TPM
 - W tym trybie do uruchomienia wymagane jest podanie hasła lub wykorzystanie klucza USB.
- Uwierzytelnianie za pomocą TPM
 - "Wymagane" włącza tryb tylko TPM, w którym klucze szyfrowania są przechowywane w układzie TPM. Użytkownik będzie uzyskać dostęp bez konieczności podawania kodu PIN lub klucza startowego podczas uruchamiania.
- Uwierzytelnianie za pomocą TPM i klucza startowego
 - Jeśli używany TPM wraz z kluczem USB, informacje potrzebne do zaszyfrowania dysku są przechowywane na kluczu USB. Po włożeniu klucza USB do urządzenia próba uzyskania dostępu do dysku jest uwierzytelniana i dysk staje się dostępny.
- Uwierzytelnianie za pomocą TPM i PIN

- To ustawienie pozwala skonfigurować, czy BitLocker ma wymagać dodatkowego uwierzytelniania przy każdym uruchomieniu komputera i czy używasz TPM (Trusted Platform Module).
- Uwierzytelnianie za pomocą TPM, klucza startowego i PIN
 - Wymagany domyślnie sposób autoryzacji jeśli TPM jest niedostępny

Funkcjonalność

Pozwalaj używać aparatu

- Polityka pozwala na korzystanie z aparatu. Jeśli jest odznaczona, aparat nie będzie działał w żadnych aplikacjach, w tym w aplikacji Proget.

Usługi lokalizacji

- Polityka określa, czy urządzenie może korzystać z usług lokalizacji.

Dane mobilne

- Polityka określa, czy urządzenie może korzystać z danych mobilnych.

Pozwalaj na VPN przez dane mobilne

- Polityka określa, czy VPN na urządzeniu może korzystać z danych mobilnych.

Roaming danych mobilnych

- Polityka określa, czy urządzenie może korzystać z danych mobilnych w roamingu.

Pozwalaj na VPN przez dane mobilne w roamingu

- Polityka określa, czy VPN na urządzeniu może korzystać z danych mobilnych w roamingu.

Pozwalaj używać kart SD

- Polityka określa, czy na urządzeniu można korzystać z karty pamięci SD.

Pozwalaj pokazywać powiadomienia na zablokowanym ekranie

- Polityka określa, czy urządzenie może wyświetlać powiadomienia w panelu powiadomień na zablokowanym ekranie urządzenia.

Pozwalaj używać sieci Wi-Fi

- Polityka określa, czy na urządzeniu można korzystać z modułu sieci Wi-Fi.

Pozwalaj na udostępnianie Wi-Fi

- Polityka pozwala na udostępnianie sieci Wi-Fi.

Pozwalaj ręcznie konfigurować sieci Wi-Fi

- Polityka określa, czy na urządzeniu można dodawać własne sieci bezprzewodowe Wi-Fi.

Pozwalaj na zmianę ustawień daty i czasu

- Polityka pozwala użytkownikowi na zmianę daty i czasu na urządzeniu.

Bezpieczeństwo

Pozwalaj na wykrywanie urządzenia przez inne urządzenia za pomocą Bluetooth

- Polityka określa, czy urządzenie może być wykrywane przez inne urządzenia za pomocą Bluetooth.

Pozwalaj na usunięcie konta "Praca"

- Polityka określa czy na urządzeniu może zostać usunięte konto praca (odłączenie urządzenia od systemu MDM).

Pozwalaj na przywrócenie urządzenia do ustawień fabrycznych

- Polityka określa czy urządzenie może zostać przywrócone do ustawień fabrycznych przez użytkownika.

Hasło aplikacji Proget

- Hasło należy podać przy odinstalowaniu aplikacji Proget z urządzenia użytkownika.

Profile

Zaktualizowano: 16 lip 2026

Aby korzystać w pełni z funkcjonalności naszego systemu, należy skonfigurować podstawowe profile, niezbędne do zapoznania się z tym w jaki sposób możemy dodawać konta pocztowe, lokalizować urządzenie, zarządzać aplikacjami poprzez białą i czarną listę, dostarczać do urządzenia niezbędne dokumenty firmowe takie jak: kontakty czy pliki. Warto również zabezpieczyć się na wypadek utraty danych wykonując kopię zapasową.



ActiveSync

Automatyczna konfiguracja synchronizacji poczty z serwerem...



APN

Konfiguracja dostępu do internetu, MMS lub WAP przez APN



Apple Business Manager

Automatyczna aktywacja urządzeń Apple przez Apple Business Manager



Apple Update

Konfiguracja harmonogramu i opóźnień aktualizacji iOS i macOS



Reguły aplikacji

Zarządzanie regułami uprawnień instalacji aplikacji



Kopia zapasowa

Kopia zapasowa kontaktów, SMS/MMS i dziennika połączeń



Kontakty służbowe

Przesyłanie pliku kontaktów służbowych na urządzenia



Dokumenty firmowe

Udostępnianie dokumentów firmowych do pobrania na urządzeniach



Certyfikat

Wysyłanie certyfikatu na urządzenie w celu autoryzacji hosta



Mapowanie certyfikatu

Powiązanie certyfikatu lub profilu SCEP z konkretnym adresem URL



Łączność

Konfiguracja połączeń, SMS-ów i transmisji danych mobilnych



Custom Apple Configuration

Stosowanie niestandardowej konfiguracji dla urządzeń Apple



Geofencing

Akcje zależne od lokalizacji urządzenia i stref służbowych



IMAP/POP

Łączenie z serwerami pocztowymi przez IMAP lub POP



Kiosk

Ograniczenie urządzenia do jednej lub kilku aplikacji



Lokalizacja

Monitorowanie i wyświetlanie lokalizacji urządzenia na mapie



Urządzenie współdzielone

Zmiana użytkowników na współdzielonym urządzeniu bez...



MTP

Wykrywanie zagrożeń urządzenia i reakcje bezpieczeństwa



SCEP

Automatyczne wnioskowanie o certyfikat bez poświadczeń...



VPN

Łączenie urządzenia z lokalną siecią firmową



Tapeta

Personalizacja obrazu ekranu głównego i blokady



Wi-Fi

Definiowanie zaufanych sieci Wi-Fi i bezpiecznej autoryzacji

ActiveSync

Zaktualizowano: 3 cze 2026

Profil ActiveSync pozwala automatycznie skonfigurować profil pocztowy na urządzeniu, w celu połączenia się z serwerem pocztowym Microsoft Exchange i synchronizacji danych tj. poczta email, kalendarz, kontakty.

Kompatybilność:

- iOS

- Windows

Przestarzała

* Name:

Example

Domain:

Example

Gateway:

None

Port:

443

* Email server:

mail.example.com

Synchronization time frame:

1 day

Synchronization interval:

Automatic - Push

Authentication:

Password

Certificate:

Select

SCEP profile:

Select

* Email:

{User:Email}

* Username:

{User:Name}

Account name:

{User:DisplayName}

☐ Use OAuth for Authentication

OAuth Sign in URL:

OAuth Token Request URL:

☒ Use SSL

☐ Accept all SSL certificates

☐ Sync Calendar

☐ Synchronize contacts

☐ Automatic sync in roaming

☐ Allow edit account settings

S/MIME

☐ Use S/MIME

☐ Always sign emails with a S/MIME certificate

☐ Default encrypt emails with a S/MIME certificate

☐ Ask the user whether to encrypt message

1 Name

- Wpisz nazwę profilu ActiveSync
- Maksymalna długość tekstu to 255
- Wymagane

2.1 Domena

- Wpisz nazwę domeny serwera Exchange
- Maksymalna długość tekstu to 32

2.2 Gateway

- Wybierz profil Gateway z listy, który zabezpieczy ruch pomiędzy urządzeniem mobilnym a wewnętrznymi systemami e-mail

2.3 Port

- Wpisz numer portu protokołu, za pomocą którego następuje połączenie z usługą (domyślnie używany jest port 443 do połączenia za pomocą TLS / SSL)
- Maksymalna wartość to 65535
- Wymagane

2.4 Serwer e-mail

- Wpisz nazwę serwera, na którym utworzono konto
- Maksymalna długość tekstu to 32
- Wymagane

2.5 Okres synchronizacji

- Określa, z jakiego przedziału czasowego będą synchronizowane dane
- Jedna z:
 - 1 dzień
 - Tydzień
 - 2 tygodnie
 - Miesiąc
 - Wszystkie

2.6 Interwał synchronizacji

- Określa częstotliwość synchronizacji danych (Automatyczny lub Przedział czasu)
- Jedna z:
 - Automatyczny - Push
 - Nigdy
 - 5 minut
 - 10 minut
 - 30 minut
 - 1 godzina

2.7 Uwierzytelnienie

- Wybierz hasło do uwierzytelniania
- Jedna z:
 - Hasło
 - Certyfikat
 - Profil SCEP

2.8 Certyfikat

- Wybierz profil certyfikatu, który będzie używany do uwierzytelniania

2.9 Profil SCEP

- Wybierz profil SCEP, który będzie używany do uwierzytelniania

3 Konfiguracja Użytkownika

3.1 E-mail

- Wpisz adres e-mail, dla którego zostanie skonfigurowany profil
- Dostępne zmienne globalne
- Maksymalna długość tekstu to 255
- Wymagane

3.2 Nazwa użytkownika

- Nazwa użytkownika pasująca do nazwy konta w Exchange
- Dostępne zmienne globalne
- Maksymalna długość tekstu to 32
- Wymagane

3.3 Nazwa konta

- Dostępne zmienne globalne
- Maksymalna długość tekstu to 32

3.4 Używaj OAuth do uwierzytelniania

- Jeśli zaznaczone, pozwala użytkownikowi na automatyczną autoryzację
- Dostępne tylko na urządzeniach z iOS 12.0 lub wyższym

3.5 URL logowania OAuth

- URL do punktu końcowego, który uwierzytelnia dane użytkownika
- Dostępne tylko na urządzeniach z iOS 12.0 lub wyższym
- Dostępne jeśli zaznaczono "Używaj OAuth do uwierzytelniania"
- Maksymalna długość tekstu to 512

3.6 URL żądania tokenu OAuth

- Tokeny autoryzacji do potwierdzania tożsamości między konsumentami a dostawcami usług
- Dostępne tylko na urządzeniach z iOS 12.0 lub wyższym
- Dostępne jeśli zaznaczono "Używaj OAuth do uwierzytelniania"
- Maksymalna długość tekstu to 512

4

Konfiguracja Bezpieczeństwa

4.1 Używaj SSL

- Jeśli zaznaczone, używanie SSL podczas łączenia jest dozwolone. Zapewnia to, że połączenie jest zabezpieczone certyfikatem SSL.

4.2 Akceptuj wszystkie certyfikaty SSL

- Jeśli zaznaczone, wszystkie certyfikaty dla połączenia zostaną zaakceptowane

4.3 Synchronizuj kalendarz

- Jeśli zaznaczone, dane kalendarza zostaną pobrane podczas synchronizacji konta

4.4 Synchronizuj kontakty

- Jeśli zaznaczone, kontakty zostaną pobrane podczas synchronizacji konta

4.5 Synchronizuj automatycznie w roamingu

- Jeśli zaznaczone, dane konta Exchange będą automatycznie synchronizowane (z określonym interwałem) także przy użyciu danych roamingowych, co może skutkować dodatkowymi opłatami

4.6 Pozwalaj edytować ustawienia konta

- Jeśli zaznaczone, zmiana ustawień konta z aplikacji będzie dozwolona

4.7 Używaj S/MIME

- Jeśli zaznaczone, poczta zostanie zaszyfrowana według standardu S/MIME

4.8 Zawsze podpisuj certyfikatem S/MIME

- Jeśli zaznaczone, maile zawsze będą podpisane certyfikatem S/MIME. Zapewnia to, że wiadomość w skrzynce odbiorczej jest dokładnie tą wiadomością, która została wysłana przez nadawcę.

- Dostępne jeśli zaznaczono "Używaj S/MIME"

4.9 Domyślnie szyfruj certyfikatem S/MIME

- Jeśli zaznaczone, maile będą szyfrowane certyfikatem S/MIME. Zapewnia to, że treść wiadomości zostanie pokazana tylko osobom z odpowiednim kluczem.
- Dostępne jeśli zaznaczono "Używaj S/MIME"

4.10 Zapytaj użytkownika, czy szyfrować wiadomość

- Jeśli zaznaczone, użytkownik ma możliwość wyboru, czy wiadomość powinna być zaszyfrowana
- Dostępne jeśli zaznaczono "Używaj S/MIME"

APN

Zaktualizowano: 3 cze 2026

Konfiguracja APN zapewnia dostęp do Internetu lub opcjonalnie dostęp do usług typu MMS lub WAP.

Kompatybilność:

- Android Enterprise Device Owner
 - Android Enterprise Profile Owner (COPE)
 - iOS
-

* Name:

Example



Android Enterprise configuration ⓘ



Samsung configuration



iOS configuration

1 Nazwa

- Wpisz nazwę profilu APN
- Maksymalna długość tekstu to 255
- Wymagane

2 Konfiguracja Android Enterprise

3 Konfiguracja Samsung

4 Konfiguracja iOS

Konfiguracja Android Enterprise

Zaktualizowano: 3 gru 2024

Konfiguracja APN zapewnia dostęp do Internetu lub opcjonalnie dostęp do usług typu MMS lub WAP.

* APN:

internet

Type of credentials:

PAP



* MCC:

260

* MNC:

06

* Name:

Example APN configuration

Carrier ID:

User:

Password:



* APN type: ⓘ

Default



MVNO type:

Select



Network type:

Select



Protocol:

Select



Roaming protocol:

Select



Proxy settings:

Proxy server address:

Proxy server port:

MMS:

MMSC:

MMS proxy server address:

MMS proxy server port:

1 APN

- Wpisz nazwę punktu dostępu (APN)
- Maksymalna długość tekstu to 255 znaków
- Wymagane

2 Rodzaj poświadczenia

- Jedno z:
 - PAP
 - CHAP
 - PAP lub CHAP

3 MCC

- Wpisz kod kraju sieci komórkowej (MCC)
- Numer trzycyfrowy
- Wymagane

4 MNC

- Wpisz kod sieci komórkowej (MNC)
- Numer dwu- lub trzycyfrowy
- Wymagane

5 Nazwa

- Wpisz nazwę APN
- Maksymalna długość tekstu to 255 znaków
- Wymagane

6 ID Operatora

- Wpisz identyfikator operatora w platformie Android

7 Użytkownik

- Wpisz nazwę użytkownika
- Maksymalna długość tekstu to 255 znaków

8 Hasło

- Wpisz hasło użytkownika
- Maksymalna długość tekstu to 255 znaków

9 Typ APN

- Dostępne opcje:

- Default
- Emergency
- CBS
- FOTA
- DUN
- MMS
- MCX
- IA
- IMS
- SUPL
- HIPRI
- XCAP

- Wymagane

10 Typ MVNO

- Jedno z:

- SPM
- IMSI
- GID
- ICCID

11 Typ sieci

- Dostępne opcje:

- Unknown
- GPRS
- EDGE
- CDMA
- EVDO_0

- EVDO_A
- 1xRTT
- HSDPA
- HSUPA
- HSPA
- EVDO_B
- IDEN
- LTE
- EHRDP
- HSPAP
- GSM
- TD_SCDMA
- IWLAN
- NR

12 Protokół

- Jedno z:
 - IP
 - IPv6
 - IPv4v6
 - PPP
 - Non IP
 - Unstructured

13 Protokół roamingu

- Jedno z:
 - IP
 - IPv6
 - IPv4v6

- PPP
- Non IP
- Unstructured

14 Adres serwera proxy

- Wpisz adres serwera proxy
- Maksymalna długość tekstu to 255 znaków

15 Port serwera proxy

- Wpisz port serwera proxy
- Maksymalna wartość to 65535

16 MMSC

- Wpisz adres Centrum Wiadomości Multimedialnych (MMSC)
- Maksymalna długość tekstu to 255 znaków

17 Adres serwera proxy MMS

- Wpisz adres serwera proxy dla MMS
- Maksymalna długość tekstu to 255 znaków

18 Port serwera proxy MMS

- Wpisz port serwera proxy MMS
- Maksymalna wartość to 65535

Konfiguracja Samsung

Zaktualizowano: 3 gru 2024

Konfiguracja APN zapewnia dostęp do Internetu lub opcjonalnie dostęp do usług typu MMS lub WAP.

* APN:

internet

* Name:

Example APN configuration

Type of credentials:

PAP



* MCC:

260

* MNC:

06

User:

Password:



Server address:



Set as preferred ⓘ

Proxy settings:

Proxy server address:

Proxy server port:

MMS:

MMSC:

MMS proxy server address: _____

MMS proxy server port: _____

1 APN

- Wpisz nazwę punktu dostępu (Access Point Name)
- Maksymalna długość tekstu to 255
- Wymagane

2 Nazwa

- Wpisz nazwę APN
- Maksymalna długość tekstu to 255
- Wymagane

3 Rodzaj poświadczenia

- Jeden z:
 - PAP
 - CHAP
 - PAP lub CHAP

4 MCC

- Wpisz kod kraju (Mobile Country Code)
- Numer trzycyfrowy
- Wymagane

5 MNC

- Wpisz kod sieci komórkowej (Mobile Network Code)
- Numer dwu lub trzycyfrowy
- Wymagane

6 Użytkownik

- Wpisz nazwę użytkownika
- Maksymalna długość tekstu to 255

7 Hasło

- Wpisz hasło użytkownika
- Maksymalna długość tekstu to 255

8 Adres serwera

- Wpisz adres serwera
- Maksymalna długość tekstu to 255

9 Ustaw jako preferowany

- Jeśli zaznaczone, nowy preferowany APN urządzenia zostanie nadpisany poprzednim preferowanym APN

10 Adres serwera proxy

- Wpisz adres serwera proxy
- Maksymalna długość tekstu to 255

11 Port serwera proxy

- Wpisz port serwera proxy
- Maksymalna wartość to 65535

12 MMSC

- Wpisz MMSC (Multimedia Messaging Service Center)
- Maksymalna długość tekstu to 255

13 Adres serwera proxy MMS

- Wpisz adres serwera proxy usługi MMS (Multimedia Messaging Service)
- Maksymalna długość tekstu to 255

14 Port serwera proxy MMS

- Wpisz port serwera proxy usługi MMS (Multimedia Messaging Service)
- Maksymalna wartość to 65535

15 SUPL

- Jeśli zaznaczone, APN ustanawia bezpieczne połączenie z serwerem lokalizacyjnym w sieci operatora

Konfiguracja iOS

Zaktualizowano: 3 gru 2024

Konfiguracja APN zapewnia dostęp do Internetu lub opcjonalnie dostęp do usług typu MMS lub WAP.

Type of APN configuration:

Default APN



Default APN

* APN:

internet

Type of credentials:

PAP



User:

Password:



Data APN

APN:

Type of credentials:

PAP



User:

Password:



Proxy server address:

Proxy server port:

1 Typ konfiguracji APN

- Wybierz rodzaj konfiguracji APN
- Jeden z:
 - Domyślny APN
 - Data APN
 - Domyślny APN i Data APN

2 Domyślny APN - APN

- Wpisz nazwę punktu dostępu Domyślnego APN
- Maksymalna długość tekstu to 255
- Wymagane jeśli wybrano "Domyślny APN" lub "Domyślny APN i Data APN"

3 Domyślny APN - Rodzaj poświadczenia

- Jeden z:
 - PAP
 - CHAP

4 Domyślny APN - Użytkownik

- Wpisz nazwę użytkownika Domyślnego APN
- Maksymalna długość tekstu to 255

5 Domyślny APN - Hasło

- Wpisz hasło użytkownika Domyślnego APN
- Maksymalna długość tekstu to 255

6 Data APN - APN

- Wpisz nazwę punktu dostępu Data APN

- Maksymalna długość tekstu to 255
- Wymagane jeśli typ konfiguracji APN to "Data APN" lub "Domyślny APN i Data APN"

7 APN - Rodzaj poświadczenia

- Jeden z:
 - PAP
 - CHAP
- Dostępne jeśli wybrano "Domyślny APN" lub "Domyślny APN i Data APN"

8 Data APN - Użytkownik

- Wpisz nazwę użytkownika Data APN
- Maksymalna długość tekstu to 255
- Dostępne jeśli wybrano "Domyślny APN" lub "Domyślny APN i Data APN"

9 Data APN - Hasło

- Wpisz hasło użytkownika Data APN
- Maksymalna długość tekstu to 255
- Dostępne jeśli wybrano "Domyślny APN" lub "Domyślny APN i Data APN"

10 Adres serwera proxy

- Wpisz adres serwera proxy
- Maksymalna długość tekstu to 255
- Dostępne jeśli wybrano "Domyślny APN" lub "Domyślny APN i Data APN"

11 Port serwera proxy

- Wpisz port serwera proxy
- Maksymalna wartość to 65535
- Dostępne jeśli wybrano "Domyślny APN" lub "Domyślny APN i Data APN"

1 Nazwa

- Nazwa profilu Apple Business Manager
- Maksymalna długość tekstu to 255
- Wymagane

2 Podstawowe informacje

2.1 Departament IT

- Nazwa działu, która będzie wyświetlana w ustawieniach zarządzanego profilu
- Maksymalna długość tekstu to 125
- Wymagane

2.2 Telefon kontaktowy

- Numer telefonu wsparcia
- Maksymalna długość tekstu to 32
- Wymagane

2.3 Oznacz jako profil domyślny

- Jeśli zaznaczone, profil zostanie automatycznie dodany do wszystkich nowo dostarczonych urządzeń przez Apple Business Manager
- Może być tylko jeden domyślny profil

3 Ustawienia profilu MDM

3.1 Pozwalaj usuwać profil MDM

- Jeśli zaznaczone, użytkownik będzie mógł ręcznie usunąć profil MDM
- Wymagany tryb nadzorowany

3.2 Pozwalaj parować urządzenie z hostem (np. iTunes)

- Jeśli zaznaczone, użytkownik będzie mógł sparować urządzenie Apple z hostem, takim jak iTunes

3.3 Certyfikat hosta

- Jeśli wybrane, urządzenie będzie kontynuować parowanie z hostem, który posiada jeden z tych certyfikatów

Ustawienia pierwszego uruchomienia

4 MacOS i iOS

4.1 Pomiń ekran Wybierz swój wygląd

- Jeśli zaznaczone, ekran wyboru Twojego ekranu blokady zostanie pominięty
- Dostępne w iOS 13 lub nowszym
- Dostępne w macOS 10.14 lub nowszym

4.2 Pomiń panel App Store

- Jeśli zaznaczone, panel App Store zostanie pominięty
- Dostępne w iOS 14.3 lub nowszym
- Dostępne w macOS 11.1 lub nowszym

4.3 Pomiń ustawienia serwisów lokalizacyjnych

- Jeśli zaznaczone, ustawienia serwisów lokalizacyjnych zostaną pominięte
- Dostępne w iOS 7 lub nowszym
- Dostępne w macOS 10.11 lub nowszym

4.4 Pomiń ustawienia przywracania i kopii zapasowej

- Jeśli zaznaczone, ustawienia przywracania i tworzenia kopii zapasowych zostaną pominięte
- Dostępne w iOS 7 lub nowszym
- Dostępne w macOS 10.9 lub nowszym

4.5 Pomiń ustawienia Apple ID oraz iCloud

- Jeśli zaznaczone:
 - Ustawienia Apple ID oraz iCloud zostaną pominięte
 - Ustawienia Apple Pay zostaną automatycznie wyłączone
- Dostępne w iOS 7 lub nowszym
- Dostępne w macOS 10.9 lub nowszym

4.6 Pomiń warunki i zasady

- Jeśli zaznaczone, Regulamin i Warunki zostaną pominięte
- Dostępne w iOS 7 lub nowszym
- Dostępne w macOS 10.9 lub nowszym

4.7 Pomiń ustawienia asystenta głosowego Siri

- Jeśli zaznaczone, ustawienia Siri zostaną pominięte
- Dostępne w iOS 7 lub nowszym
- Dostępne w macOS 10.12 lub nowszym

4.8 Pomiń ustawienia wysyłania informacji diagnostycznych

- Jeśli zaznaczone, ustawienia diagnostyczne zostaną pominięte
- Dostępne w iOS 7 lub nowszym
- Dostępne w macOS 10.9 lub nowszym

4.9 Pomiń ustawienia odcisku palca

- Jeśli zaznaczone:
 - Ustawienia Touch ID zostaną pominięte
 - Ustawienia Apple Pay zostaną automatycznie wyłączone
- Dostępne w iOS 8.1 lub nowszym
- Dostępne w macOS 10.12.4 lub nowszym

4.10 Pomiń ustawienia Apple Pay

- Jeśli zaznaczone, konfiguracja Apple Pay zostanie pominięta
- Dostępne w iOS 8.1 lub nowszym
- Dostępne w macOS 10.12.4 lub nowszym

4.11 Pomiń ekran prywatności

- Jeśli zaznaczone, ekran Prywatność zostanie pominięty
- Dostępne w iOS 11.13 lub nowszym
- Dostępne w macOS 10.13.4 lub nowszym

4.12 Pomiń ekran czasu ekranu

- Jeśli zaznaczone, ekran Czas przed ekranem zostanie pominięty
- Dostępne w iOS 12 lub nowszym
- Dostępne w macOS 10.15 lub nowszym

5 Tylko iOS

5.1 Pomiń panel migracji urządzenia do urządzenia

- Jeśli zaznaczone, panel migracja z urządzenia do urządzenia zostanie pominięty
- Dostępne w iOS 13+
- Dostępne w iOS 13 lub nowszym

5.2 Pomiń panel iMessage

- Jeśli zaznaczone, panel iMessage zostanie pominięty
- Dostępne w iOS 10 lub nowszym

5.3 Pomiń panel Ukończono przywracanie

- Jeśli zaznaczone, panel Zakończono Przywracanie zostanie pominięty
- Dostępne w iOS 14 lub nowszym

5.4 Pomiń panel Ukończono aktualizację oprogramowania

- Jeśli zaznaczone, panel Zakończono Aktualizację Oprogramowania zostanie pominięty
- Dostępne w iOS 14 lub nowszym

5.5 Pomiń panel Startowy

- Jeśli zaznaczone, panel Rozpocznij zostanie pominięty
- Dostępne w iOS 13 lub nowszym

5.6 Pomiń ustawienia

- Jeśli zaznaczone, ustawienia "Przenieś z Androida" zostaną pominięte
- Dostępne w iOS 9 lub nowszym

5.7 Pomiń tworzenie hasła urządzenia

- Jeśli zaznaczone:

- Tworzenie hasła urządzenia zostanie pominięte
- Ustawienia Apple Pay i ustawienia Touch ID zostaną automatycznie wyłączone
- Dostępne w iOS 7 lub nowszym

5.8 Pomiń ustawienia trybu wyświetlania ekranu startowego

- Jeśli zaznaczone, ustawienia trybu wyświetlania ekranu startowego zostaną pominięte
- Dostępne w iOS 8.3 lub nowszym

5.9 Pomiń ekran migracji Apple Watch

- Jeśli zaznaczone, ekran migracji Apple Watch zostanie pominięty
- Dostępne w iOS 11 lub nowszym

5.10 Pomiń ekran iMessage i FaceTime

- Jeśli zaznaczone, ekran iMessage i FaceTime zostanie pominięty
- Dostępne w iOS 12 lub nowszym

5.11 Pomiń ekran obowiązkowej aktualizacji oprogramowania

- Jeśli zaznaczone, ekran obowiązkowej aktualizacji oprogramowania zostanie pominięty
- Dostępne w iOS 12 lub nowszym

5.12 Pomiń ekran Dodaj plan komórkowy

- Jeśli zaznaczone, ekran Dodaj plan komórkowy zostanie pominięty
- Dostępne w iOS 12 lub nowszym

6 Tylko MacOS

6.1 Pomiń panel ułatwień dostępu

- Jeśli zaznaczone, panel ułatwień dostępu zostanie pominięty
- Dostępne w macOS 11 lub nowszym

6.2 Pomiń ekran iCloud Analytics

- Jeśli zaznaczone, ekran iCloud Analytics zostanie pominięty
- Dostępne w macOS 10.12.4 lub nowszym

6.3 Pomiń panel Odblokowanie Mac za pomocą Apple Watch

- Jeśli zaznaczone, panel Odblokowanie Mac za pomocą Apple Watch zostanie pominięty
- Dostępne w macOS 12 lub nowszym

6.4 Pomiń ekran ustawień FileVault dla urządzeń OS X

- Jeśli zaznaczone, ekran ustawień FileVault dla urządzeń OS X zostanie pominięty
- Dostępne w macOS 10.10 lub nowszym

6.5 Pomiń ustawienia iCloud Storage

- Jeśli zaznaczone, ustawienia w iCloud Storage zostaną pominięte
- Dostępne w macOS 10.13.4 lub nowszym

Apple Update

Zaktualizowano: 3 cze 2026

Profil Apple Update umożliwia konfigurację ustawień aktualizacji systemu iOS oraz macOS. Pozwala określić m.in. harmonogram instalacji, opóźnienia aktualizacji oraz zasady ich pobierania. Aby profil działał prawidłowo, na urządzeniu musi być włączone zarządzanie deklaratywne (Declarative Management).

Kompatybilność:

- iOS (from iOS 17)
 - macOS (from macOS 14)
-

Add new Apple Update profile

* Name:

Example Apple Update profile

* Type:

Force latest version



URL address:

https://support.apple.com/guide/iphone/update-ios-iph3e504502/ios

* Days from release:

10

* Force install time:

23:00



Force installation date:

Version: ⓘ

Build version:

Back

Submit

1 Nazwa

- Wprowadź nazwę profilu Apple Update
- Maksymalna długość tekstu to 255
- Wymagane

2 Typ

- Wybierz typ aktualizacji urządzenia, taki jak:
 - Wymuś najnowszą wersję
 - Urządzenie zostanie zaktualizowane do najnowszej dostępnej wersji oprogramowania, niezależnie od aktualnie zainstalowanej
 - Określona wersja
 - Umożliwia wskazanie konkretnej wersji oprogramowania, do której urządzenie ma zostać zaktualizowane

3 Adres URL

- Podaj adres URL strony internetowej z dodatkowymi informacjami dla użytkowników na temat wymuszonej aktualizacji oprogramowania

4 Dni od wydania

- Określ liczbę dni od wydania aktualizacji, po których instalacja zostanie automatycznie wymuszona na urządzeniu
- Dostępne po wybraniu opcji **Wymuś najnowszą wersję**
- Wymagane

5 Wymuś czas instalacji

- Ustaw lokalną godzinę, o której instalacja aktualizacji oprogramowania zostanie wymuszona
- Dostępne po wybraniu opcji **Wymuś najnowszą wersję**
- Wymagane

6 Wymuś datę instalacji

- Ustaw lokalną datę, w której instalacja aktualizacji oprogramowania zostanie wymuszona (format RFC3339, bez przesunięcia strefy czasowej)
- Dostępne po wybraniu opcji **Określona wersja**
- Wymagane

7 Wersja

- Wybierz docelową wersję systemu operacyjnego, do której urządzenie ma zostać zaktualizowane
- Dostępne po wybraniu opcji **Określona wersja**
- Wymagane

- Wprowadź docelową wersję kompilacji systemu (build), która ma zostać zainstalowana na urządzeniu
- Dostępne po wybraniu opcji **Określona wersja**

Reguły aplikacji

Zaktualizowano: 3 cze 2026

Profil Reguły aplikacji umożliwia dodawanie reguł, które będą zarządzały uprawnieniami dotyczącymi instalacją aplikacji na urządzeniach użytkownika. Blokowanie systemowych aplikacji może skutkować nieprawidłowym działaniem lub uszkodzeniem urządzenia.

Kompatybilność:

- Android Enterprise Device Owner
 - Android Enterprise Profile Owner
 - iOS (Tryb nadzorowany)
-

* Name:

Example

ⓘ Adding apps to the profile will not force their installation on the device. The view below is for illustrative purposes only. Only the package name is taken into account and the icon and name of the application may differ on the device.

Android Enterprise - work space Android Enterprise - private space iOS (supervisor mode)

1 Nazwa

- Wprowadź nazwę profilu Reguł Aplikacji
- Maksymalna długość tekstu to 255
- Wymagane

2 Android Enterprise - przestrzeń służbowa

3 Android Enterprise - przestrzeń prywatna

4 iOS (Tryb nadzorowany)

Android Enterprise - przestrzeń służbowa

Zaktualizowano: 3 gru 2024

Profil Reguły aplikacji umożliwia dodawanie reguł, które będą zarządzały uprawnieniami dotyczącymi instalacją aplikacji na urządzeniach użytkownika. Blokowanie systemowych aplikacji może skutkować nieprawidłowym działaniem lub uszkodzeniem urządzenia.

UNLOCK APPS

Package Id: Start typing...

Reset filters

Selected: 0

Deselect all

☐	ICON	APP NAME	PACKAGE ID
No data available			

Results: 0

Clear list

Add application manually

Add applications from system

BLACKLIST

☐ Block all apps

Package Id: Start typing...

Reset filters

Selected: 0

Deselect all

☐	ICON	APP NAME	PACKAGE ID
No data available			

Results: 0

Clear list

Add application manually

Add applications from system

1 Odblokuj aplikacje

1.1 Wyczyść listę

- Usuwa wszystkie aplikacje dodane do listy

1.2 Dodaj aplikację ręcznie

- Dodaj aplikację do profilu zasad aplikacji, podając jej ID pakietu

1.3 Dodaj aplikacje z systemu

- Dodaj aplikacje z listy dostępnych aplikacji w systemie

2 Czarna lista

2.1 Zablokuj wszystkie aplikacje

- Jeśli zaznaczone, blokuje wszystkie aplikacje na urządzeniu z wyjątkiem aplikacji Proget, Ustawień i Google Play

2.2 Wyczyść listę

- Usuwa wszystkie aplikacje dodane do listy

2.3 Dodaj aplikację ręcznie

- Dodaj aplikację do profilu zasad aplikacji, podając jej ID pakietu

2.4 Dodaj aplikacje z systemu

- Dodaj aplikacje z listy dostępnych aplikacji w systemie

Android Enterprise - przestrzeń prywatna

Zaktualizowano: 3 gru 2024

Profil Reguły aplikacji umożliwia dodawanie reguł, które będą zarządzały uprawnieniami dotyczącymi instalacją aplikacji na urządzeniach użytkownika. Blokowanie systemowych aplikacji może skutkować nieprawidłowym działaniem lub uszkodzeniem urządzenia.

Available for COPE activation

WHITELIST

Package id: Start typing...

Reset filters

Selected: 0 | Deselect all

☐	ICON	APP NAME	PACKAGE ID
No data available			

Results: 0

Clear list

Add application manually

Add applications from system

BLACKLIST

Package id: Start typing...

Reset filters

Selected: 0 | Deselect all

☐	ICON	APP NAME	PACKAGE ID
No data available			

Results: 0

Clear list

Add application manually

Add applications from system

1 Biała lista

1.1 Wyczyść listę

- Usuwa wszystkie aplikacje dodane do listy

1.2 Dodaj aplikację ręcznie

- Dodaj aplikację do profilu reguł aplikacji, podając jej identyfikator pakietu

1.3 Dodaj aplikacje z systemu

- Dodaj aplikacje z listy dostępnych aplikacji w systemie

2 Czarna lista

2.1 Wyczyść listę

- Usuwa wszystkie aplikacje dodane do listy

2.2 Dodaj aplikację ręcznie

- Dodaj aplikację do profilu reguł aplikacji, podając jej identyfikator pakietu

2.3 Dodaj aplikacje z systemu

- Dodaj aplikacje z listy dostępnych aplikacji w systemie

iOS (Tryb nadzorowany)

Zaktualizowano: 3 gru 2024

Profil Reguły aplikacji umożliwia dodawanie reguł, które będą zarządzały uprawnieniami dotyczącymi instalacją aplikacji na urządzeniach użytkownika. Blokowanie systemowych aplikacji może skutkować nieprawidłowym działaniem lub uszkodzeniem urządzenia.

WHITELIST

Package id: Start typing...

Reset filters

Selected: 0

Deselect all

ICON

APP NAME

PACKAGE ID

No data available

Results: 0

<<

<

1

>

>>

Clear list

Add application manually

Add applications from system

Add default applications

BLACKLIST

Package id: Start typing...

Reset filters

Selected: 0

Deselect all

ICON

APP NAME

PACKAGE ID

No data available

Results: 0

<<

<

1

>

>>

Clear list

Add application manually

Add applications from system

1

Biała lista

1.1 Wyczyść listę

- Usuwa wszystkie aplikacje dodane do listy

1.2 Dodaj aplikację ręcznie

- Dodaj aplikację do profilu reguł aplikacji, podając jej identyfikator pakietu

1.3 Dodaj aplikacje z systemu

- Dodaj aplikacje z listy dostępnych aplikacji w systemie

1.4 Dodaj aplikacje domyślne

- Dodaj aplikacje domyślne do profilu reguł aplikacji

2 Czarna lista

2.1 Wyczyść listę

- Usuwa wszystkie aplikacje dodane do listy

2.2 Dodaj aplikację ręcznie

- Dodaj aplikację do profilu reguł aplikacji, podając jej identyfikator pakietu

2.3 Dodaj aplikacje z systemu

- Dodaj aplikacje z listy dostępnych aplikacji w systemie

Kopia zapasowa

Zaktualizowano: 3 cze 2026

Profil Kopia zapasowa umożliwia stworzenie kopii zapasowej kontaktów, SMS i MMS oraz dziennika połączeń. Podczas konfiguracji profilu można określić elementy oraz częstotliwość wykonywania kopii zapasowej.

Kompatybilność:

- Android
- Android Enterprise Profile Owner
- Android Enterprise Device Owner

* Name:

Example

BACKUP ITEMS

☒ Make a backup of contacts

☒ Make a copy of SMS / MMS ⓘ

☒ Make a backup of call log

☒ Allow the use of mobile data

FREQUENCY

Frequency of sending (in days, 1-30):

1

* What time?:

12:00

DELETING COPIES

☒ Delete backup

Older than (in days, 1-365):

30

1 Nazwa

- Wprowadź nazwę profilu kopii zapasowej
- Maksymalna długość tekstu to 255
- Wymagane

2 Elementy Kopii Zapasowej

2.1 Wykonuj kopię zapasową kontaktów

- Jeśli zaznaczone, umożliwia utworzenie kopii kontaktów z urządzenia

2.2 Wykonuj kopię SMS/MMS

- Jeśli zaznaczone, umożliwia utworzenie kopii SMS / MMS z urządzenia

2.3 Wykonuj kopię zapasową dziennika połączeń

- Jeśli zaznaczone, umożliwia utworzenie kopii dziennika połączeń z urządzenia

2.4 Zezwalaj na wykorzystanie danych mobilnych

- Jeśli zaznaczone, zezwala na używanie danych komórkowych do tworzenia kopii zapasowej

3 Częstotliwość

3.1 Częstotliwość wysyłania (w dniach, 1-30)

- Umożliwia ustawienie częstotliwości tworzenia kopii zapasowych co określoną liczbę dni

3.2 O której godzinie?

- Wprowadź godzinę, o której będzie wysyłana kopia zapasowa
- Wymagane

4 Usuwanie Kopii

4.1 Usuwaj kopię zapasową

- Jeśli zaznaczone, usuwa stare kopie zapasowe po określonym czasie

4.2 Starszą niż (w dniach, 1-365)

- Wybierz czas w dniach, po którym poprzednie kopie zapasowe zostaną usunięte

Kontakty służbowe

Zaktualizowano: 3 cze 2026

Profil kontaktów służbowych pozwala na przesłanie pliku kontaktów na urządzenie użytkownika.

Kompatybilność:

- Android
- Android Enterprise Profile Owner
- Android Enterprise Device Owner

* Name:

Example

☐

From a file

☐

Managed from a file

1

Name

- Wprowadź nazwę nowego profilu kontaktów służbowych
- Maksymalna długość tekstu to 255
- Wymagane

2

Z pliku

2.1 Plik VCF

- Nazwa przesłanego pliku

2.2 Wybierz plik

- Dozwolony typ pliku: VCF
- Maksymalny rozmiar pliku to 10 MB
- Wymagane

3 Zarządzane z pliku

3.1 Wybierz plik

- Dozwolone typy plików: VCF, CSV
- Maksymalny rozmiar pliku to 10 MB

3.2 Filtr

- Wprowadź znak, aby znaleźć kontakt

3.3 Usuń

- Usuwa wybrany kontakt z listy

3.4 Dodaj kontakt

- Dodaj nowy kontakt

4

Dodaj kontakt

4.1 Imię

- Wprowadź imię nowego kontaktu
- Maksymalna długość tekstu to 64
- Wymagane, jeśli pole 'Nazwisko' jest puste

4.2 Nazwisko

- Wprowadź nazwisko nowego kontaktu
- Maksymalna długość tekstu to 64
- Wymagane, jeśli pole 'Imię' jest puste

4.3 Firma

- Wprowadź nazwę firmy nowego kontaktu
- Maksymalna długość tekstu to 64

4.4 Dział

- Wprowadź nazwę działu nowego kontaktu
- Maksymalna długość tekstu to 64

4.5 Stanowisko

- Wprowadź stanowisko nowego kontaktu
- Maksymalna długość tekstu to 64

4.6 Numer telefonu 1

- Wprowadź pierwszy numer telefonu nowego kontaktu
- Maksymalna długość tekstu to 32
- Wymagane

4.7 Numer telefonu 2

- Wprowadź drugi numer telefonu nowego kontaktu
- Maksymalna długość tekstu to 32

4.8 Email

- Wprowadź adres E-mail nowego kontaktu
- Maksymalna długość tekstu to 255

5 Edycja

5.1 Filtr

- Wprowadź znak, aby znaleźć kontakt

5.2 Usuń

- Usuwa wybrane kontakty
- Usunięty kontakt zostanie przeniesiony do listy zmodyfikowanych kontaktów ze statusem 'Usunięty'

5.3 Dodaj kontakt

- Dodaj nowy kontakt

5.4 Edytuj

- Edytuj wybrane kontakty
- Edytowany kontakt zostanie przeniesiony do listy zmodyfikowanych kontaktów ze statusem 'Edytowany'

5.5 Usuń

- Usuń wybrane kontakty
- Usunięty kontakt zostanie przeniesiony do listy zmodyfikowanych kontaktów ze statusem 'Usunięty'

6 Przy usunięciu kontaktu

6.1 Usuń

- Usuń wybrane kontakty z listy zmodyfikowanych kontaktów

6.2 Edytuj

- Edytuj wybrany kontakt z listy zmodyfikowanych kontaktów

6.3 Usuń

- Usuń wybrany kontakt z listy zmodyfikowanych kontaktów

Dokumenty firmowe

Zaktualizowano: 3 cze 2026

Profil Dokumenty firmowe umożliwia wgranie dokumentów na serwer, które zostaną udostępnione do pobrania na urządzeniach użytkownika, który posiada ten profil.

Kompatybilność:

- Android
- Android Enterprise Profile Owner
- Android Enterprise Device Owner

Name: ⓘ

Example

☒ Allow downloading files via Wi-Fi wireless network

☒ Allow downloading files via data transmission

☐ Notify changes

☐ Add files to the Downloads folder ⓘ

☐ Download files automatically

BUSINESS DOCUMENTS

Example directory

Selected: 0 | Deselect all

Create directory

Upload files

	NAME	SIZE	CREATION DATE
☐	Example directory	Elements: 0	-
☐	example.vcf	708 B	2024-09-05 02:08:24

1

Nazwa

- Wprowadź nazwę profilu dokumentów firmowych
- Maksymalna długość tekstu to 255
- Wymagane

2

Konfiguracja

2.1 Pozwalaj pobierać pliki za pośrednictwem sieci bezprzewodowej Wi-Fi

- Jeśli zaznaczone, pobieranie plików przez Wi-Fi jest dozwolone

2.2 Pozwalaj pobierać pliki za pośrednictwem transmisji danych

- Jeśli zaznaczone, pobieranie plików przez transmisję danych jest dozwolone

2.3 Powiadamiaj o zmianach

- Jeśli zaznaczone, użytkownik zostanie poinformowany o zmianach w profilu dokumentów firmowych

2.4 Dodaj pliki do folderu Pobrane

- Jeśli zaznaczone, pliki będą dodane do folderu Pobrane na urządzeniu

2.5 Pobieraj pliki automatycznie

- Jeśli zaznaczone, pliki zostaną automatycznie pobrane na urządzeniu

3 Katalog

3.1 Katalog

- Kliknij, aby wyświetlić katalog

3.2 Pobierz

- Pobierz wybrany plik

3.3 Zmień nazwę

- Zmień nazwę wybranego pliku lub katalogu

3.4 Usuń

- Usuń wybrany plik lub katalog

3.5 Dodaj folder

- Dodaj nowy folder

3.6 Wyślij pliki

- Wyślij plik z komputera

Certyfikat

Zaktualizowano: 8 cze 2026

Profil Certyfikat umożliwia wysłanie dowolnego certyfikatu do urządzenia mobilnego w celu autoryzacji hosta.

Kompatybilność:

- Android
 - Android Enterprise Device Owner
 - Android Enterprise Profile Owner
 - iOS
 - macOS
-

* Name:

Example

☐ File

☐ Template

☐ SCEP

1 Nazwa

- Wprowadź nazwę profilu certyfikatu
- Maksymalna długość tekstu to 255
- Wymagane

2 Plik

- Jeśli wybrane, profil certyfikatu jest tworzony poprzez wgranie pliku certyfikatu

3 Szablon

- Jeśli wybrane, profil certyfikatu jest tworzony na podstawie szablonu

4 SCEP

NOWOŚĆ

- Jeśli wybrane, profil certyfikatu jest tworzony poprzez konfigurację serwera SCEP

Plik

Zaktualizowano: 8 cze 2026

Opcja Plik pozwala wgrać do profilu gotowy plik certyfikatu z systemu. Skorzystaj z tej opcji, gdy posiadasz już wygenerowany certyfikat (np. wystawiony przez zewnętrzny urząd certyfikacji), który chcesz dystrybuować na urządzenia. Obsługiwane formaty plików: .crt, .cer, .der, .pfx, .p12. Jeśli certyfikat jest zabezpieczony hasłem, należy je podać podczas przesyłania.

File

Certificate: ⓘ

example.cer - 1.04 KiB (1.06 KB)

Select file

Password:

☒ Certificate for Windows activation ⓘ

* Certificate type:

CA x v

1 Certyfikat

- Wybrana nazwa pliku
- Wymagane

2 Wybierz plik

- Wybierz plik z systemu, który zostanie użyty w profilu
- Dozwolony typ pliku: .crt, .cer, .der, .pfx, .p12

3 Hasło

- Wprowadź hasło do certyfikatu
- Wymagane, jeśli certyfikat jest zabezpieczony hasłem

4 Certyfikat dla aktywacji Windows

NOWOŚĆ

- Po zaznaczeniu tej opcji, wgrany certyfikat w profilu zostanie zainstalowany na urządzeniu z aktywacją Windows
- Dotyczy wyłącznie urządzeń Windows
- Dozwolone rozszerzenia pliku certyfikatu w systemie Windows to: .pem, .crt, .cer, .der

5 Typ certyfikatu

NOWOŚĆ

- Wybierz typ certyfikatu, który określa sposób jego wykorzystania na urządzeniu
- Dostępne opcje: CA, Intermediate
- To pole jest dostępne wyłącznie po zaznaczeniu opcji 'Certyfikat dla aktywacji Windows'

Szablon

Zaktualizowano: 9 cze 2026

Szablon to konfiguracja, która automatycznie generuje certyfikaty, gdy urządzenie ich potrzebuje. Wymaga certyfikatu CA utworzonego w Menedżerze Certyfikatów. Można również dodać niestandardowe atrybuty, które są wbudowywane w CSR, oraz skonfigurować automatyczne odnawianie przed wygaśnięciem certyfikatu.

Template

* CA:

CA

* Key length:

2048

* Encryption signature:

SHA-256

* Scope:

User

* Validity (in days):

365

* Common Name:

{User:Email}

☒ Auto renew

Specify the time before the occurrence of the event in which the certificate should be renewed (in days, 1-14):

3

TYPE	* VALUE	ACTIONS
NT_principal_Name	Value	

Clear

Add

1 Certyfikat CA

- Wybierz certyfikat CA, który został utworzony w Menedżerze Certyfikatów. Jest używany do weryfikacji tożsamości certyfikatu.
- Wymagane

2 Długość klucza

- Wybierz długość klucza. Określa, jak silne będzie zabezpieczenie.
- Wymagane

3 Podpis szyfrujący

- Wybierz rodzaj algorytmu haszującego. Określa, jak silne będzie zabezpieczenie.
- Wymagane

4 Zakres

- Wybierz zakres certyfikatu, taki jak:

- Użytkownik
- Urządzenie
- Wymagane

5 Ważność (w dniach)

- Określ, jak długo certyfikat będzie ważny
- Minimalna wartość to 30
- Maksymalna wartość to 730
- Wymagane

6 Common Name

- Wprowadź CN certyfikatu. Jest to charakterystyczna wartość certyfikatu.
- Dostępne zmienne globalne
- Wymagane

7 Automatyczne odnawianie

- Jeśli zaznaczone, certyfikat zostanie odnowiony x dni przed końcem jego ważności

8 Czas przed odnowieniem certyfikatu

- Określ, ile dni przed końcem ważności certyfikatu powinno nastąpić jego odnowienie

9 Typ

- Wybierz typ niestandardowych atrybutów, które są fragmentami danych wbudowanymi tylko w CSR.

10 Wartość

- Wprowadź wartość typu
- Dostępne zmienne globalne

11 Usuń

- Usuń wybrany niestandardowy atrybut

12 Wyczyść

- Usuń wszystkie niestandardowe atrybuty

13 Dodaj

- Dodaj niestandardowy atrybut

SCEP

Zaktualizowano: 9 cze 2026

NOWOŚĆ

Certyfikat typu SCEP konfiguruje możliwość automatycznego wnioskowania o certyfikat użytkownika lub urządzenia w celu autoryzacji klienta bez podawania poświadczeń domenowych.

SCEP

* Access address:

Example access address

* Encryption Algorithm:

AES-256

CA ID:

* Encryption signature:

SHA-256

* Subject:

{User:Email}

* Key length:

2048

* Fingerprint:

Example fingerprint

* Password:

.....

* Scope:

User

☐ Key encipherment
 ☐ Digital signature
 ☐ Microsoft User Security

☒ Auto renew

Specify the time before the occurrence of the event in which the certificate should be renewed (in days, 1-14):

3

TYPE	* VALUE	ACTIONS
NT_principal_Name	Example value	

Clear

Add

1

Konfiguracja SCEP

1.1 Adres dostępowy

- Wprowadź nazwę URL dla serwera SCEP (np. Network Device Enrollment Service)
- Domyślnie obsługiwany jest tylko port 80 (HTTP)
- Przykładowy URL: `http:///certsrv/mscep/mscep.dll`
- Maksymalna długość tekstu to 255
- Wymagane

1.2 Identyfikator CA

- Wprowadź nazwę profilu dla serwerów SCEP (np. Network Device Enrollment Service), które obsługują profile nazwane.
- Maksymalna długość tekstu to 255

1.3 Temat

- Dostępne zmienne globalne
- Wymagane

1.4 Odcisk palca

- Wprowadź odcisk CA wydającego certyfikat główny na serwerze SCEP (np. Network Device Enrollment Service)
- Maksymalna długość tekstu to 500
- Wymagane

1.5 Zakres

- Użytkownik
- Urządzenie

1.6 Automatyczne odnawianie

- Jeśli włączone, certyfikat zostanie automatycznie odnowiony przed wygaśnięciem

1.7 Odnów przed

- Określ czas przed wystąpieniem zdarzenia, w którym certyfikat powinien zostać odnowiony (w dniach, 1-14)
- Wartość domyślna: 3
- Dostępne gdy 'Automatyczne odnawianie' jest włączone

1.8 Algorytm szyfrowania

- Typ algorytmu szyfrowania. Określa, jak mocne będzie zabezpieczenie.
- Jedno z:
 - AES128
 - AES192
 - AES256
- Wymagane

1.9 Podpis szyfrowania

- Typ podpisu szyfrowania. Określa, jak mocne będzie zabezpieczenie.
- Jedno z:
 - SHA256
 - SHA384
 - SHA512
- Wymagane

1.10 Długość klucza

- Długość klucza. Określa, jak mocne będzie zabezpieczenie
- Jedno z:
 - 2048

- 3072
- 4096
- Wymagane

1.11 Hasło

- Wprowadź 'enrollment static password' wygenerowane podczas wdrażania serwera SCEP
- Obsługiwane jest tylko statyczne hasło
- Wartość powinna być 32-znakowym ciągiem znaków alfanumerycznych
- Maksymalna długość tekstu to 255
- Wymagane

1.12 Szyfrowanie klucza

- Jeśli zaznaczone, użyj jako szyfrowanie klucza
- Użyj, gdy nadawca i odbiorca klucza publicznego muszą wygenerować klucz bez użycia szyfrowania

1.13 Podpis cyfrowy

- Jeśli zaznaczone, użyj jako podpis cyfrowy
- Specyficzny typ podpisu, który jest wspierany przez cyfrowy certyfikat. Zapewnia dowód Twojej tożsamości

1.14 Microsoft User Security

- Jeśli zaznaczone, użyj szablonu certyfikatu Microsoft User Security

2 Alternatywne nazwy

2.1 Typ

- Jedno z:
 - Distinguished_Name
 - NT_principal_Name
 - RFC822_Name
 - DNS_Name
- Wymagane

2.2 Wartość

- Dostępne zmienne globalne
- Wymagane

2.3 Usuń

- Usuwa dodaną nazwę alternatywną

2.4 Wyczyść

- Usuwa wszystkie dodane nazwy alternatywne z listy

2.5 Dodaj

- Dodaje nazwę alternatywną do listy

Mapowanie certyfikatu

Zaktualizowano: 3 cze 2026

Mapowanie certyfikatu pozwala na powiązanie profilu Certyfikat lub SCEP z konkretnym adresem URL. Dodanie profilu na urządzenie powoduje, że dostarczony certyfikat zostanie automatycznie wybrany przy próbie połączenia ze zdefiniowanym adresem URL, zarówno przez przeglądarkę jak i inne aplikacje.

Kompatybilność:

- Android Enterprise Profile Owner
 - Android Enterprise Device Owner
-

Add new certificate mapping profile

ⓘ Assigning a certificate to a URL takes priority over assigning a certificate to an application.

* Name:

Example

Assign Certificate to URL

Example.URL

Certificate



Add

Assign Certificate to App

Example.App

Certificate



Add

Back

Submit

1 Nazwa

- Wprowadź nazwę profilu mapowania certyfikatów
- Maksymalna długość tekstu to 255
- Wymagane

2 URL

- Wprowadź określony adres URL
- Maksymalna długość tekstu to 255
- Wymagane

3 Certyfikat

- Wybierz certyfikat autoryzujący dla wybranego adresu URL
- Wymagane

4 Usuń

- Usuwa adres URL i certyfikat

5 Dodaj URL

- Dodaj nowy adres URL

6 Aplikacja

- Wprowadź określone ID aplikacji
- Maksymalna długość tekstu to 255
- Wymagane

7 Certyfikat

- Wybierz certyfikat autoryzujący dla wybranej aplikacji
- Wymagane

8 Usuń

- Usuwa ID aplikacji i certyfikat

9 Dodaj aplikację

- Dodaj nowe ID aplikacji

Łączność

Zaktualizowano: 3 cze 2026

Profil łączności pozwala na wprowadzenie konfiguracji związanej z komunikacją wychodzącą i przychodzącą z urządzenia (połączenia, SMS) oraz wykorzystaniem danych mobilnych.

Kompatybilność:

- Android (Samsung)
- Android Enterprise Device Owner (Samsung)

Name:

Example

CONFIGURATION

MOBILE INTERNET

Allow trusted conditions only

CONNECTIONS

Incoming:

Allow trusted conditions only

Outgoing:

Allow trusted conditions only

SMS

Incoming:

Allow trusted conditions only

Outgoing:

Allow trusted conditions only

MMS

Incoming:

Allow trusted conditions only

Outgoing:

Allow trusted conditions only

TRUSTED CONDITIONS

COUNTRIES

Trust all

Trust only

Select

CONTACTS

Trust all

Trust only

Select

CONNECTIVITY RULES

Trust all operators

Trust only

MCCMNC

ACTIONS

Add

Import from file

1 Nazwa

- Wprowadź nazwę profilu łączności
- Maksymalna długość tekstu to 255
- Wymagane

2 Konfiguracje

2.1 Internet mobilny

- Określ zasady korzystania z Internetu mobilnego, takie jak:
 - Zablokuj wszystko
 - Zezwalaj na wszystko
 - Zezwalaj tylko na zaufane warunki

2.2 Połączenia przychodzące

- Określ zasady korzystania z Połączeń przychodzących, takie jak:
 - Zablokuj wszystko
 - Zezwalaj na wszystko
 - Zezwalaj tylko na zaufane warunki

2.3 Połączenia wychodzące

- Określ zasady korzystania z połączeń wychodzących, takie jak:
 - Zablokuj wszystko
 - Zezwalaj na wszystko
 - Zezwalaj tylko na zaufane warunki

2.4 SMS przychodzące

- Określ zasady korzystania z SMS-ów przychodzących, takie jak:
 - Zablokuj wszystko
 - Zezwalaj na wszystko
 - Zezwalaj tylko na zaufane warunki

2.5 SMS wychodzące

- Określ zasady korzystania z SMS-ów wychodzących, takie jak:
 - Zablokuj wszystko

- Zezwalaj na wszystko
- Zezwalaj tylko na zaufane warunki

2.6 MMS przychodzące

- Określ zasady korzystania z MMS-ów przychodzących, takie jak:
 - Zablokuj wszystko
 - Zezwalaj na wszystko
 - Zezwalaj tylko na zaufane warunki

2.7 MMS wychodzące

- Określ zasady korzystania z MMS-ów wychodzących, takie jak:
 - Zablokuj wszystko
 - Zezwalaj na wszystko
 - Zezwalaj tylko na zaufane warunki

3 Zaufane warunki

3.1 Kraje

- Wybierz kraje, dla których będą obowiązywać zaufane warunki, jeśli wybrano opcję 'Zaufaj tylko'

3.2 Kontakty

- Wybierz kontakty, dla których będą obowiązywać zaufane warunki, jeśli wybrano opcję 'Zaufaj tylko'

3.3 Dodaj reguły łączności

- Ręcznie dodaj reguły łączności z kodami MCC i MNC, dla których będą obowiązywać zaufane warunki, jeśli wybrano opcję 'Zaufaj tylko'

3.4 Importuj reguły łączności z pliku

- Importuj z pliku reguły łączności z kodami MCC i MNC, dla których będą obowiązywać zaufane warunki, jeśli wybrano opcję 'Zaufaj tylko'

3.5 Przykładowy plik CSV

- Pobierz na swoje urządzenie przykładowy plik CSV z kodami MCC i MNC

Custom Apple Configuration

Zaktualizowano: 3 cze 2026

Custom Apple Configuration zawiera payload z ustawieniami, kontami, poświadczeniami itp. dla urządzeń Apple. Custom Apple Configuration umożliwia zastosowanie niestandardowej konfiguracji dla urządzeń Apple, które nie są jeszcze obecne w bieżącej wersji serwera Proget. Aby utworzyć Custom Apple Configuration należy zapoznać się z dokumentacją Apple lub Proget.

Kompatybilność:

- iOS
 - macOS
-

* Name:

Example

* Channel:

User

* Configuration: ⓘ

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4   <dict>
5     <key>PayloadVersion</key>
6     <integer>1</integer>
7     <key>PayloadUUID</key>
8     <string>Ignored</string>
9     <key>PayloadType</key>
10    <string>Configuration</string>
11    <key>PayloadIdentifier</key>
12    <string>Ignored</string>
13    <key>PayloadContent</key>
14    <array>
15      <dict>
16        <key>PayloadContent</key>
17        <dict>
18          <key>URL</key>
19          <string>https://scep.example.com/scep</string>
20          <key>Name</key>
21          <string>EnrollmentCAInstance</string>
22          <key>Subject</key>
```

1 Nazwa

- Wprowadź nazwę konfiguracji
- Maksymalna długość tekstu to 125
- Wymagane

2 Kanał

- Wybierz kanał dla konfiguracji:
 - Urządzenie
 - Użytkownik
- Wymagane

3 Konfiguracja

- Wprowadź konfigurację XML lub przeciągnij i upuść plik tutaj.
- Wymagane

Geofencing

Zaktualizowano: 3 cze 2026

Geofencing pozwala na dostosowanie konfiguracji i restrykcji do urządzeń na podstawie lokalizacji. Profil umożliwia konfigurację określonych akcji w strefach służbowych jak i poza nimi.

Kompatybilność:

- Android Enterprise Profile Owner
- Android Enterprise Device Owner

1. Mapa Geofencing

Name:

Example

GEOFENCING ZONES

Selected: 0

•••

At least one zone is required

Add new zone

EVENTS OUTSIDE THE ZONE

Assign profiles

Lock Device

Wipe company data

Wipe device

Send event notification

+

-

© OpenStreetMap contributors

- Wprowadź nazwę nowego profilu Geofencing
 - Maksymalna długość tekstu to 255
 - Wymagane
-

2. Strefy Geofencing

1 Edytuj

- Edytuj wybraną strefę

2 Usuń

- Usuń wybraną strefę

3 Utworzone strefy

- Lista utworzonych stref

4 Konfiguracja nowej strefy

4.1 Nazwa

- Wprowadź nazwę strefy
- Wymagane

4.2 Szerokość geograficzna

- Wprowadź szerokość geograficzną strefy
- Wymagane

4.3 Długość geograficzna

- Wprowadź długość geograficzną strefy
- Wymagane

4.4 Zasięg

- Wprowadź zasięg strefy
- Wymagane

4.5 Znajdź miejsce

- Znajdź miejsce na mapie

3. Zdarzenia

1 Przypisz polityki

1.1 Wybierz polityki

- Wybierz polityki, które zostaną przypisane podczas zdarzenia

2 Przypisz profile

2.1 Wybierz profile

- Wybierz profile, które zostaną przypisane podczas zdarzenia

3 Zablokuj urządzenie

3.1 Tolerancja

- Wybierz czas, po którym urządzenie zostanie zablokowane

3.2 Wiadomość

- Wprowadź wiadomość, która zostanie wyświetlona na zablokowanym ekranie

3.3 Numer telefonu

- Wprowadź numer telefonu, który zostanie wyświetlony na zablokowanym ekranie

4 Wyczyścić dane służbowe

4.1 Tolerancja

- Wybierz czas, po którym urządzenie wyczyści dane służbowe

5 Wyczyść dane urządzenia

5.1 Tolerancja

- Wybierz czas, po którym wszystkie dane urządzenia zostaną wyczyszczone

6 Wyślij powiadomienie o zdarzeniu

6.1 Pole tekstowe

- Wprowadź tekst, który zostanie wyświetlony w powiadomieniach na urządzeniach poza strefą

IMAP/POP

Zaktualizowano: 3 cze 2026

Profil IMAP/POP określa sposób łączenia się z serwerami pocztowymi poprzez protokół IMAP lub POP w celu synchronizacji danych tj. poczta email.

Kompatybilność:

- iOS
- macOS

* Name:	Example		
* Email:	{User:Email}	INBOUND SERVER DATA	OUTGOING SERVER DATA
* Account name:	{User:DisplayName}	* Server address: example@address.com	* Server address: example@address.com
* Message sender:	{User:Name}	* User name: {User:Name}	* User name: {User:Name}
Account type:	IMAP ▼	Password: 👁️	Password: 👁️
☐ Set as default		Type of security: None ▼	Type of security: None ▼
☐ Enable notifications		* Port: 143	* Port: 587

1 Nazwa

- Nazwa nowego profilu IMAP/POP
- Maksymalna długość tekstu to 255
- Wymagane

2 Dane e-mail

2.1 E-mail

- Wprowadź adres e-mail, dla którego zostanie skonfigurowany profil
- Dostępne zmienne globalne
- Maksymalna długość tekstu to 255
- Wymagane

2.2 Nazwa konta

- Wprowadź nazwę konta, która będzie widoczna w aplikacji klienta e-mail na urządzeniu mobilnym
- Dostępne zmienne globalne
- Maksymalna długość tekstu to 128
- Wymagane

2.3 Nadawca wiadomości

- Dostępne zmienne globalne
- Maksymalna długość tekstu to 128
- Wymagane

2.4 Typ konta

- Jeden z:
 - POP
 - IMAP

2.5 Ustaw jako domyślne

- Jeśli zaznaczone, konto zostanie ustawione jako domyślne konto pocztowe na urządzeniu

2.6 Włącz powiadomienia

- Jeśli zaznaczone, powiadomienia dotyczące poczty będą wyświetlane na urządzeniu

3

Dane serwera przychodzącego

3.1 Adres serwera

- Wprowadź adres serwera e-mail, który będzie używany do wysyłania wiadomości
- Maksymalna długość tekstu to 255
- Wymagane

3.2 Nazwa użytkownika

- Wprowadź nazwę użytkownika e-maila, który będzie używany do wysyłania wiadomości
- Maksymalna długość tekstu to 128
- Wymagane

3.3 Hasło

- Wprowadź hasło do e-maila, który będzie używany do wysyłania wiadomości
- Wymagane

3.4 Typ zabezpieczeń

- Jeden z:
 - Brak
 - SSL/TLS
 - SSL/TLS (Akceptuj wszystkie certyfikaty)
 - STARTTLS
 - STARTTLS (Akceptuj wszystkie certyfikaty)

3.5 Port

- Wprowadź numer portu
- Wymagane

4

Dane serwera wychodzącego

4.1 Adres serwera

- Wprowadź adres serwera e-mail, który będzie używany do wysyłania wiadomości
- Maksymalna długość tekstu to 255
- Wymagane

4.2 Nazwa użytkownika

- Wprowadź nazwę użytkownika poczty e-mail, która będzie używana do wysyłania wiadomości
- Maksymalna długość tekstu to 128
- Wymagane

4.3 Hasło

- Wprowadź hasło do e-maila, który będzie używany do wysyłania wiadomości
- Wymagane

4.4 Typ zabezpieczeń

- Jeden z:
 - Brak
 - SSL/TLS
 - SSL/TLS (Akceptuj wszystkie certyfikaty)
 - STARTTLS
 - STARTTLS (Akceptuj wszystkie certyfikaty)

4.5 Port

- Wprowadź numer portu
- Wymagane

Kiosk

Zaktualizowano: 3 cze 2026

Profil Kiosk pozwala ograniczyć korzystanie z urządzenia tylko do określonych aplikacji. Możesz użyć profilu Kiosk, aby skonfigurować urządzenie do korzystania tylko z jednej lub kilku konkretnych aplikacji.

Kompatybilność:

- Android Enterprise Device Owner
- iOS (Tryb nadzorowany)

Add new Kiosk profile

* Name:

Example

Compatibility Android

Compatibility iOS

1 Nazwa

- Wprowadź nazwę profilu Kiosku
- Maksymalna długość tekstu to 255
- Wymagane

2 Kompatybilność Android

3 Kompatybilność iOS

Android

Zaktualizowano: 3 cze 2026

Profil Kiosk umożliwia ograniczenie funkcjonalności urządzenia do określonych aplikacji. Za pomocą profilu Kiosk można skonfigurować urządzenie do korzystania tylko z jednej lub kilku określonych aplikacji.

Compatibility Android

Compatibility iOS

☒ Disable volume adjustment ⓘ

☒ Disable navigation buttons ⓘ

☒ Do not turn off the screen while charging ⓘ

☒ Disable notifications ⓘ

☒ Disable status bar ⓘ

ⓘ Available only on devices where a password requirement policy is not set.

☒ Display Kiosk above the lock screen

Force a kiosk:

Do not force ▼

* PIN: ⓘ

1234

☒ Allow access to settings on the Kiosk exit screen

Manage settings

Kiosk Mode

☐ Single app

☐ Multi app

1 Konfiguracja

1.1 Zablokuj regulację głośności

- Jeśli zaznaczone, przyciski głośności zostaną wyłączone podczas włączonego Kiosku

1.2 Wyłącz przyciski nawigacji

- Jeśli zaznaczone, blokuje używanie przycisków „Recent Apps”, „Home” i „Back” podczas włączonego Kiosku
- Dostępne tylko dla Device Owner Android Enterprise

1.3 Nie wyłączaj ekranu podczas ładowania

- Jeśli zaznaczone, ekran nie wyłączy się podczas ładowania, gdy Kiosk jest włączony

1.4 Blokuj powiadomienia

- Jeśli zaznaczone, zabrania używania przycisku Home podczas włączonego Kiosku
- Dostępne tylko na urządzeniach z Androidem 9.0 lub wyższym
- Dostępne tylko dla Device Owner Android Enterprise

1.5 Blokuj pasek stanu

- Jeśli zaznaczone, blokuje dostęp do paska stanu urządzenia, po odznaczeniu urządzenie wyświetli informacje takie jak status baterii, połączenie z siecią Wi-Fi, zegar
- Dostępne tylko na urządzeniach z Androidem 9.0 lub wyższym
- Dostępne tylko dla Device Owner Android Enterprise

1.6 Wyświetlaj Kiosk nad ekranem blokady

NOWOŚĆ

- Jeśli zaznaczone, Kiosk będzie wyświetlany nad ekranem blokady
- Domyślnie Kiosk wyświetla się pod ekranem blokady
- Działa wyłącznie wtedy, gdy polityka hasła nie wymaga jego podania

- Dostępne tylko dla Device Owner Android Enterprise

1.7 Wymuś nałożenie Kiosku

- Określa, czy i po jakim czasie profil Kiosku pojawi się na urządzeniu (np. jeśli użytkownik go zamknął)
- Jedna z opcji:
 - Nie wymuszaj
 - 5
 - 10
 - 15
 - 30
 - 60

1.8 PIN

- Wpisz PIN, który będzie używany do wyjścia z kiosku
- Minimalna długość PIN-u to 4
- Maksymalna długość PIN-u to 16
- Wymagane

1.9 Zezwól na dostęp do ustawień na ekranie wyjścia z kiosku

NOWOŚĆ

- Jeśli zaznaczone, użytkownik będzie miał dostęp do panelu ustawień Proget (np. Wi-Fi, głośność, jasność) na ekranie wyjścia z kiosku
- Ekran wyjścia z kiosku jest dostępny po kilkukrotnym kliknięciu przycisku "Wstecz"
- Dostępne w trybie kiosku 'Wiele aplikacji' oraz 'Pojedyncza aplikacja'
- Dostępne tylko dla Device Owner Android Enterprise

1.10 Zarządzaj ustawieniami

NOWOŚĆ

- Konfiguruj, które kategorie ustawień będą dostępne na ekranie wyjścia z kiosku
 - Wi-Fi
 - Pokaż dostępne sieci
 - Połączenia Wi-Fi
 - Bluetooth
 - Sieci Mobilne
 - Jasność ekranu
 - Głośność
- Jeśli ustawione, wymaga przynajmniej jednej kategorii
- Dostępne gdy zaznaczono "Zezwól na dostęp do ustawień na ekranie wyjścia z kiosku"

2 Pojedyncza aplikacja

3 Wiele aplikacji

Pojedyncza aplikacja

Zaktualizowano: 7 maj 2026

Profil Kiosk umożliwia ograniczenie funkcjonalności urządzenia do określonych aplikacji. Za pomocą profilu Kiosk można skonfigurować urządzenie do korzystania tylko z jednej lub kilku określonych aplikacji.

ⓘ Adding apps to the profile will not force their installation on the device. The view below is for illustrative purposes only. Only the package name is taken into account and the icon and name of the application may differ on the device.

APP

Package Id:

[Reset filters](#) [BASIC](#) [PQL](#)

Selected: 0 | [Deselect all](#) 

☐	ICON	APP NAME	PACKAGE ID
☐		Gmail	com.google.android.gm

[Clear list](#) [Add application manually](#) [Add applications from system](#)

HIDDEN APPS: ⓘ

Package Id:

[Reset filters](#) [BASIC](#) [PQL](#)

Selected: 0 | [Deselect all](#) 

 No data available
Data has not been entered yet.

[Clear list](#) [Add application manually](#) [Add applications from system](#)

1 Usuń

- Usuwa aplikację dodaną do listy

2 Lista aplikacji

- Szczegóły aplikacji dodanej do kiosku

3 Wyczyść listę

- Usuwa wszystkie aplikacje dodane do listy

4 Dodaj aplikację ręcznie

- Dodaj aplikację do kiosku, podając jej ID pakietu

5 Dodaj aplikacje z systemu

- Dodaj aplikacje z listy dostępnych aplikacji w systemie

6 Ukryte aplikacje

- Dodaj aplikacje ręcznie lub z systemu, które chcesz ukryć

1

Konfiguracja administratora

1.1 Wymagane logowanie

- Jeśli zaznaczone, wymaga zalogowania się do kiosku za pomocą danych uwierzytelniających serwisu
- Dostępne tylko dla aktywacji Device Owner Android Enterprise

1.2 Użytkownik serwisowy

- Wpisz nazwę użytkownika serwisu kiosku
- Wymagane jeśli zaznaczono 'Wymagane logowanie'

1.3 PIN serwisowy

- Wpisz hasło serwisu kiosku
- Wymagane jeśli zaznaczono 'Wymagane logowanie'

1.4 Zapamiętywanie loginu

- Wybierz z rozwijanej listy:
 - Wymuś
 - Pozwól
 - Zabroń

1.5 Automatyczne wylogowanie

NOWOŚĆ

- Jeśli włączone, użytkownik zostanie automatycznie wylogowany z kiosku po wygaszeniu ekranu
- Jeśli wyłączone, dedykowana akcja wylogowania staje się dostępna bezpośrednio na ekranie kiosku
- Dostępne tylko dla aktywacji Device Owner Android Enterprise
- Dostępne gdy zaznaczono 'Wymagane logowanie'

1.6 Czas automatycznego wylogowania

NOWOŚĆ

- Określ czas po wygaszeniu ekranu, po którym użytkownik ma zostać automatycznie wylogowany
- Wartość domyślnie ustawiona na 'Natychmiastowe'
- Dostępne gdy włączono 'Automatyczne wylogowanie'

2 Dostosowanie nagłówka

2.1 Wyświetl nagłówek

- Jeśli zaznaczone, wyświetla nagłówek w kiosku
- Dostępne tylko dla aktywacji Device Owner Android Enterprise

2.2 Logo

- Wybierz plik z logo w kiosku
- Dozwolony typ pliku: png
- Wymagana kwadratowa grafika o maksymalnych wymiarach 192 x 192 px

2.3 Kolor nagłówka

- Wybierz kolor tła nagłówka ekranu

2.4 Kolor tekstu nagłówka

- Wybierz kolor tekstu nagłówka ekranu

2.5 Tekst nagłówka

- Wpisz tekst nagłówka ekranu
- Maksymalna długość to 24

3 Konfiguracja launchera

3.1 Kolor tekstu aplikacji

- Wybierz kolor tekstu aplikacji w kiosku
- Dostępne tylko dla aktywacji Device Owner Android Enterprise

3.2 Kolor tła / tapeta

- Dostępne tylko dla aktywacji Device Owner Android Enterprise

3.3 Kolor

- Wybierz kolor tła ekranu launchera
- Dostępne tylko dla aktywacji Device Owner Android Enterprise

3.4 Tapeta

- Wybierz plik tapety w kiosku
- Dozwolony typ pliku: png

3.5 Orientacja

- Jedna z:
 - Automatyczna
 - Pionowa
 - Pozioma

4 Aplikacje

4.1 Siatka

- Wybierz siatkę aplikacji w Kiosku
- Dostępne rozmiary zależą od wybranej orientacji

4.2 Miejsce aplikacji

- Dodaj aplikacje do ekranu

4.3 Dodaj aplikację ręcznie

- Dodaj aplikację do kiosku, podając jej ID pakietu

4.4 Dodaj aplikacje z systemu

- Dodaj aplikacje z listy dostępnych aplikacji w systemie

4.5 Dodaj ustawienia

- Ograniczony dostęp do ustawień systemowych
 - Wi-Fi
 - Pokaż dostępne sieci
 - Połączenia Wi-Fi
 - Bluetooth
 - Sieci Mobilne
 - Jasność ekranu
 - Głośność
- Jeśli ustawione, wymaga przynajmniej jednej kategorii
- Może być umieszczone w wielu miejscach na ekranie

4.6 Dodaj akcję

- Nazwa

- Ustaw nazwę akcji
- Wymagane
- Określ typ akcji, taki jak: **NOWOŚĆ**
 - Intent
 - Funkcjonalność pozwala na uruchomienie podanej akcji, za pomocą intentu
 - Intent
 - Wprowadź akcję intentu, która ma zostać uruchomiona
 - Wymagane
 - Typ akcji
 - Jedna z:
 - Uruchom aktywność
 - Uruchom usługę
 - Wyślij broadcast
 - Domyślnie: Uruchom aktywność
 - ID aplikacji
 - Wprowadź nazwę pakietu aplikacji, do której intent ma być skierowany
 - Opcjonalne
 - Dodatkowe parametry
 - Opcjonalna lista parametrów (extras) przekazywanych wraz z intentem
 - Każdy parametr wymaga:
 - Klucz
 - Typ - jeden z: String, Integer, Boolean, Float, Double
 - Wartość
 - Dodanie akcji może zezwolić użytkownikowi na przełączanie się pomiędzy widokami aplikacji, do których nie powinien mieć dostępu. Aby uruchomić intent, aplikacja, która ją obsługuje musi być odblokowana w kiosku
 - Wyloguj **NOWOŚĆ**
 - Wylogowuje użytkownika z kiosku

- Dostępne tylko gdy włączono 'Wymagane logowanie'
- Wyjdź z kiosku **NOWOŚĆ**
 - Pozwala użytkownikowi opuścić kiosk
 - Wymaga podania PIN-u serwisowego, aby potwierdzić wyjście

4.7 Dodaj ekran

- Do 8 ekranów

4.8 Usuń

- Usuwa ekran

5 Ukryte aplikacje

5.1 Usuń

- Usuwa aplikacje dodane do listy

5.2 Dodana aplikacja

- Aplikacja dodana do listy

5.3 Wyczyść listę

- Usuwa wszystkie aplikacje dodane do listy

5.4 Dodaj aplikację ręcznie

- Dodaj aplikację do kiosku, podając jej ID pakietu

5.5 Dodaj aplikacje z systemu

- Dodaj aplikacje z listy dostępnych aplikacji w systemie

ios

Zaktualizowano: 3 gru 2024

Profil Kiosku pozwala ograniczyć funkcjonalność urządzenia do określonych aplikacji. Możesz użyć profilu Kiosku, aby skonfigurować urządzenie do używania tylko jednej lub kilku określonych aplikacji.

Compatibility Android
Compatibility iOS

☐ Disable volume adjustment

☒ Disable touch

☐ Disable Screen rotation

☒ Disable Ringer switch

☐ Disable Sleep/Wake button

☐ Disable Auto Lock

☐ Enable VoiceOver

☐ Enable Zoom

☐ Enable Invert Colors

☐ Enable AssistiveTouch

☐ Enable Speak Selection

☐ Enable Mono Audio

ⓘ Adding apps to the profile will not force their installation on the device. The view below is for illustrative purposes only. Only the package name is taken into account and the icon and name of the application may differ on the device.

APP

Package Id: Start typing...

[Reset filters](#)

Selected: 0
|
[Deselect all](#)

☰

☐	ICON	APP NAME	PACKAGE ID
☐		Gmail - Email by Google	com.google.gmail

Results: 1

<<
<
1
>
>>

Clear list

Add application manually

Add applications from system

1 Konfiguracja

1.1 Zablokuj regulację głośności

- Jeśli zaznaczone, wyłącza regulację głośności w Kiosku

1.2 Wyłącz dotyk

- Jeśli zaznaczone, wyłącza dotyk w Kiosku

1.3 Wyłącz rotację ekranu

- Jeśli zaznaczone, wyłącza rotację ekranu w Kiosku

1.4 Wyłącz zmianę dźwięków

- Jeśli zaznaczone, wyłącza zmianę dźwięków w Kiosku

1.5 Wyłącz przycisk uśpienia

- Jeśli zaznaczone, wyłącza przycisk uśpienia w Kiosku

1.6 Wyłącz automatyczną blokadę

- Jeśli zaznaczone, wyłącza automatyczną blokadę w Kiosku

1.7 Włącz VoiceOver

- Jeśli zaznaczone, włącza VoiceOver w Kiosku

1.8 Włącz Zoom

- Jeśli zaznaczone, włącza funkcję Zoom w Kiosku

1.9 Włącz odwrócone kolory

- Jeśli zaznaczone, włącza odwrócone kolory w Kiosku

1.10 Włącz AssistiveTouch

- Jeśli zaznaczone, włącza AssistiveTouch w Kiosku

1.11 Włącz Mów zaznaczone

- Jeśli zaznaczone, opcja Mów jest włączona

1.12 Włącz dźwięk mono

- Jeśli zaznaczone, włącza dźwięk mono w Kiosku

2 Aplikacja

2.1 Usuń

- Usuwa aplikacje dodane do listy

2.2 Lista aplikacji

- Szczegóły aplikacji dodanej do kiosku

2.3 Wyczyść listę

- Usuń wszystkie aplikacje dodane do listy

2.4 Dodaj aplikację ręcznie

- Dodaj aplikację do kiosku podając jej ID pakietu

2.5 Dodaj aplikacje z systemu

- Dodaj aplikacje z listy dostępnych aplikacji w systemie

Lokalizacja

Zaktualizowano: 3 cze 2026

Profil Lokalizacja określa sposób monitorowania urządzenia, odświeżania jego położenia i wyświetlania na mapie.

Kompatybilność:

- Android
- Android Enterprise Device Owner
- Android Enterprise Profile Owner

Name:
Example

LOCATION HISTORY

☒ Save History

Time period (in days, 1-90):

1

☐ Require high accuracy ⓘ

☐ Send location when initiating phone call ⓘ

☐ Require location services enabled when initiating a phone call ⓘ

LOCATION

Localization type:
Interval

Time period (in minutes, 5-1440):

5

TIME LIMITS

☐ Time limits for profile ⓘ

Monday:

☒ Off

☐ Whole day

☐ Advanced

Tuesday:

☒ Off

☐ Whole day

☐ Advanced

Wednesday:

☒ Off

☐ Whole day

☐ Advanced

Thursday:

☒ Off

☐ Whole day

☐ Advanced

Friday:

☒ Off

☐ Whole day

☐ Advanced

Saturday:

☒ Off

☐ Whole day

☐ Advanced

Sunday:

☒ Off

☐ Whole day

☐ Advanced

1

Nazwa

- Nazwa profilu lokalizacja
- Maksymalna długość tekstu to 255
- Wymagane

2

Historia lokalizacji

2.1 Przechowuj historię

- Pozwala na zapisywanie historii lokalizacji

2.2 Okres (w dniach, 1-90)

- Ustaw przedział czasu dla przechowywania historii lokalizacji
- Dostępne jeśli zaznaczono "Przechowuj historię"

2.3 Wymagaj wysokiej dokładności

- Wymagaj wysokiej dokładności
- Opcja nie jest wspierana na urządzeniach z Androidem 9.0 i wyższym

2.4 Wysyłaj lokalizację przy inicjowaniu połączenia GSM

- Opcja nie jest wspierana na urządzeniach z aktywacją Android Enterprise Profile Owner

2.5 Wymuszaj włączenie lokalizacji przy inicjowaniu połączenia GSM

- Opcja nie jest wspierana na urządzeniach z aktywacją Android Enterprise Profile Owner
- Dostępne jeśli zaznaczono "Wysyłaj lokalizację przy inicjowaniu połączenia GSM"

3 Kategoria lokalizacji

3.1 Interwał

3.1.1 Tryb lokalizacji

- Jedno z:
 - Interwał czasowy
 - W ruchu

3.1.2 Okres (w minutach, 5-1440)

- Ustaw interwał pobierania lokalizacji
- Dostępne jeśli wybrano "Tryb lokalizacji: Interwał czasowy"

3.2 W ruchu

3.2.1 Tryb lokalizacji

- Jedno z:
 - Interwał czasowy
 - W ruchu

3.2.2 Idąc (w metrach, 100-500)

- Ustaw odległość pobierania lokalizacji podczas chodzenia

3.2.3 Biegając (w metrach, 500-2000)

- Ustaw odległość pobierania lokalizacji podczas biegania

3.2.4 Jadąc (w minutach, 1-30)

- Ustaw odległość pobierania lokalizacji podczas jazdy

3.2.5 Ograniczenia w ruchu

- Jedno z:
 - Brak
 - Blokuj aplikacje

3.2.6 Określ czas tolerancji, aby wyłączyć aplikacje (w sekundach, 0-600)

- Określ czas tolerancji, po którym aplikacje zostaną wyłączone
- Dostępne jeśli wybrano "Ograniczenia podczas przemieszczania się: Blokuj aplikacje" lub "Ograniczenia w ruchu: Ukryj aplikacje"

3.2.7 Określ czas tolerancji, aby włączyć aplikacje (w sekundach, 0-600)

- Określ czas tolerancji, po którym aplikacje zostaną włączone

- Dostępne jeśli wybrano "Ograniczenia podczas przemieszczania się: Blokuj aplikacje" lub "Ograniczenia w ruchu: Ukryj aplikacje"

3.2.8 Określ prędkość poruszania się, aby zastosować regułę (km/h, 1-60)

- Określ prędkość przemieszczania się
- Dostępne jeśli wybrano "Ograniczenia podczas przemieszczania się: Blokuj aplikacje" lub "Ograniczenia w ruchu: Ukryj aplikacje"

3.2.9 Wyczyść listę

- Usuwa wszystkie aplikacje dodane do listy
- Dostępne jeśli wybrano "Ograniczenia podczas przemieszczania się: Blokuj aplikacje" lub "Ograniczenia w ruchu: Ukryj aplikacje"

3.2.10 Dodaj aplikację ręcznie

- Dodaj aplikację, którą chcesz wyłączyć z ograniczeń podczas przemieszczania się, podając jej ID aplikacji
- Dostępne jeśli wybrano "Ograniczenia podczas przemieszczania się: Blokuj aplikacje" lub "Ograniczenia w ruchu: Ukryj aplikacje"

3.2.11 Dodaj aplikacje z systemu

- Dodaj aplikacje, które chcesz wyłączyć z ograniczeń podczas przemieszczania się, z listy dostępnych aplikacji w systemie
- Dostępne jeśli wybrano "Ograniczenia podczas przemieszczania się: Blokuj aplikacje" lub "Ograniczenia w ruchu: Ukryj aplikacje"

4 Limity czasowe

4.1 Limity dla profilu

- Ograniczenia czasowe dla profilu lokalizacji pozwalają na dopasowanie pobierania lokalizacji do czasu pracy użytkownika. Zastosowanie ma czas na urządzeniu użytkownika.

4.2 Wyłączone

- Lokalizacja nie będzie pobierana w wybrane dni

4.3 Cały dzień

- Lokalizacja będzie pobierana przez cały dzień

4.4 Zaawansowane

- Ustaw specyficzny czas pobierania lokalizacji w ciągu dnia

4.5 Od

- Wybierz czas, od którego chcesz, aby lokalizacja była pobierana

4.6 Do

- Wybierz czas, do którego chcesz, aby lokalizacja była pobierana

MTP

Zaktualizowano: 9 cze 2026

Profil MTP monitoruje urządzenie i wykrywa potencjalne zagrożenia na jakie może być narażone. Dodatkowo profil pozwala na skonfigurowanie określonych reakcji na wykryte incydenty bezpieczeństwa.

Kompatybilność:

- Android
- Android Enterprise Device Owner
- Android Enterprise Profile Owner

* Name:

Example

ACTION	REACTION
Device protection	
Root: Dangerous ⓘ	Only notify user
Root: Critical ⓘ	Only notify user
Knox Warranty Bit ⓘ	Only notify user
Fake device location ⓘ	Only notify user
USB debugging enabled ⓘ	Only notify user
Developer options enabled ⓘ	Only notify user
No password on the device ⓘ	Only notify user
Application security	
Unsafe admins ⓘ	Only notify user
Installation of prohibited applications ⓘ	Only notify user
Network traffic analysis	
Device has connected to an unsecured Wi-Fi ⓘ	Only notify user
Device has connected to rogue Wi-Fi ⓘ	Only notify user
DNS change on device ⓘ	Only notify user
Proxy change on device ⓘ	Only notify user
Gateway change on device ⓘ	Only notify user
No internet on the device ⓘ	Only notify user

1 Nazwa

- Wprowadź nazwę profilu MTP
- Maksymalna długość tekstu to 255 znaków
- Wymagane

2 Ochrona urządzenia

2.1 Root: Niebezpieczne

- Na urządzeniu wykryto pliki używane do rootowania. Nie oznacza to jednak, że urządzenie zostało zrootowane. Znane są przypadki, gdy takie pliki były wcześniej zainstalowane w pamięci urządzenia.

2.2 Root: Krytyczne

- Rootowanie to proces uzyskiwania nieautoryzowanego dostępu lub podwyższonych uprawnień w systemie. Może to stworzyć luki w bezpieczeństwie, które mogą być trudne do wykrycia lub do obejścia środków bezpieczeństwa urządzenia.

2.3 Knox Warranty Bit

- Knox Warranty Bit to funkcja bezpieczeństwa, która wykrywa instalację nieoficjalnego oprogramowania na urządzeniu. Pomaga to zapobiegać złośliwym próbom dostępu do danych. Knox Warranty Bit wykrywa, czy na urządzeniu został załadowany nie-Knox kernel. Jest to bit e-fuse programowalny jednokrotnie. Jeśli na urządzeniu zainstalowano nie-Knox boot loader lub kernel, Knox nie może już zagwarantować bezpieczeństwa.

2.4 Fałszywa lokalizacja urządzenia

- Urządzenie przedstawia fałszywą lokalizację. Używanie fałszywej lokalizacji może służyć do dezorientacji systemów monitorujących urządzenie, w tym systemów przyznających dostęp do zasobów firmowych na podstawie lokalizacji urządzenia (np. geofencing). Funkcja niedostępna dla Android Enterprise Profile Owner. Funkcja wymaga użycia profilu lokalizacyjnego do prawidłowego działania.

2.5 Włączone debugowanie przez USB

- Debugowanie USB to opcja konfiguracji przeznaczona wyłącznie do celów programistycznych. Włączając debugowanie USB, urządzenie może akceptować polecenia z komputera poprzez kabel USB. Nie działa dla aktywacji Android Enterprise Profile Owner.

2.6 Włączone opcje deweloperskie

- Opcje deweloperskie to opcje konfiguracji przeznaczone wyłącznie do celów programistycznych. Po ich włączeniu, użytkownik może zmieniać zaawansowane ustawienia, co zagraża integralności konfiguracji i bezpieczeństwu urządzenia. Nie działa dla aktywacji Android Enterprise Profile Owner.

2.7 Brak hasła na urządzeniu

- Urządzenie nie jest zabezpieczone hasłem. Silne hasło chroni dane użytkownika, a także dane firmowe przed wyciekiem lub kradzieżą. Zaleca się ustawienie hasła numerycznego lub kodu PIN w celu bezpiecznego korzystania z urządzenia.

3 Bezpieczeństwo aplikacji

3.1 Niezaufani administratorzy

- Aplikacje z uprawnieniami administratora mogą częściowo kontrolować urządzenie. Najczęściej takie uprawnienia mają aplikacje do obsługi poczty, kalendarza lub inne aplikacje służbowe, które otrzymały takie uprawnienia przy dodawaniu aplikacji służbowych. Dotyczy to szczególnie aplikacji, które wymagają stosowania polityk bezpieczeństwa na urządzeniach. Jeśli aplikacja nie jest aplikacją służbową, zaleca się jej odinstalowanie.

3.2 Dodaj aplikacje domyślne

- Dodaje aplikacje z uprawnieniami administratora do kontrolowania urządzenia

3.3 Usunąć

- Usuwa bieżącą aplikację z listy dozwolonych

3.4 Instalacja niedozwolonych aplikacji

- Zainstalowano aplikację oznaczoną przez administratora jako niebezpieczną lub niepożądaną.

3.5 Usunąć

- Usuwa bieżące aplikacje z listy niedozwolonych

4 Analiza ruchu sieciowego

4.1 Urządzenie podłączyło się do niezabezpieczonej sieci Wi-Fi

- Niezabezpieczona sieć Wi-Fi jest podatna na atak sieciowy. Wymagana włączona usługa lokalizacji dla Androida 8 i nowszych.

4.2 Urządzenie podłączyło się do niezaufanej sieci Wi-Fi

- Niezaufana sieć Wi-Fi może wykorzystać podatność urządzenia na połączenie z nieznaną siecią Wi-Fi, podszywając się pod zaufaną sieć. Wymagana włączona usługa lokalizacji dla Androida 8 i nowszych.

4.3 Zaufana sieć 1

- Wprowadź SSID, aby połączyć się z bezpieczną siecią

4.4 Usuń

- Usuwa już dodaną sieć

4.5 Adres MAC

- Wprowadź poprawny adres MAC, aby dołączyć do bezpiecznej sieci
- Wymagane

4.6 Dodaj konfigurację zaufanej sieci

- Dodaje pole z nową konfiguracją bezpiecznej sieci
- Wymagane jeśli zaznaczono 'Zaufana sieć 1'

4.7 Zmiana konfiguracji DNS

- Zmiana konfiguracji DNS na urządzeniu może wskazywać, że dane są wysyłane do nieznanego miejsca docelowego (może to być próba ataku typu Man in the middle). Wymagana jest włączona usługa lokalizacji dla Androida 8 i nowszych.

4.8 Zmiana konfiguracji proxy na urządzeniu

- Zmiana konfiguracji proxy na urządzeniu może wskazywać, że dane są wysyłane do nieznanego miejsca docelowego (może to być próba ataku typu Man in the middle). Wymagana jest włączona usługa lokalizacji dla Androida 8 i nowszych.

4.9 Zmiana konfiguracji gateway

- Zmiana konfiguracji gateway na urządzeniu mobilnym może wskazywać na wysyłanie danych do nieznanego miejsca docelowego (może to być próba ataku typu Man in the middle). Wymagana jest włączona usługa lokalizacji dla Androida 8 i nowszych.

4.10 Brak internetu na urządzeniu

NOWOŚĆ

- Urządzenie nie posiada aktywnego połączenia z internetem. Brak dostępu do sieci może uniemożliwiać prawidłową komunikację z systemem MDM, odbieranie polityk bezpieczeństwa oraz instalowanie aktualizacji systemowych i aplikacyjnych.

Reakcje

1 Przełącznik

- Włącz przełącznik, aby wybrać reakcję

2 Reakcja

- Jedna z:
 - Powiadom tylko użytkownika
 - Wymaż urządzenie
 - Wymaż dane firmowe
 - Zablokuj przestrzeń służbową
 - Wyłącz Wi-Fi
 - Wyłącz Bluetooth

3 Numer telefonu

- Wprowadź numer telefonu, aby wysłać wiadomość
- Pominięcie pola sprawi, że na urządzeniu nie pojawi się przycisk 'Skontaktuj się z administratorem'
- Dostępne gdy wybrano 'Reakcja' jako 'Zablokuj przestrzeń służbową'

4 Nagłówek

NOWOŚĆ

- Zdefiniuj treść nagłówka. Jeśli pole pozostanie puste, na urządzeniu wyświetli się wartość domyślna.
- Dostępne gdy wybrano 'Reakcja' jako 'Zablokuj przestrzeń służbową'

5 Tolerancja

- Ustaw czas tolerancji przed uruchomieniem reakcji (od 15 minut do 72 godzin)
- Wymagane jeśli wybrano 'Reakcja' jako 'Zablokuj przestrzeń służbową'

6 Wiadomość

- Wprowadź treść, aby wysłać ją na wskazany numer
- Wymagane jeśli wybrano 'Reakcja' jako 'Zablokuj przestrzeń służbową'

SCEP

Zaktualizowano: 16 lip 2026

Przestarzała

[Kliknij tutaj, aby dowiedzieć się, jak utworzyć nowy typ certyfikatu](#)

Profil SCEP konfiguruje możliwość automatycznego wnioskowania o certyfikat użytkownika w celu autoryzacji klienta bez podawania poświadczeń domenowych.

Kompatybilność:

- Android Enterprise Device Owner
- Android Enterprise Profile Owner

* Name:

Example

* Access address:

Example access address

CA ID:

* Subject:

{User:Email}

* Encryption Algorithm:

AES256

* Encryption signature:

SHA256

* Key length:

2048

* Fingerprint:

Example fingerprint

* Password:

.....

☐ Key encipherment

☐ Digital signature

ALTERNATIVE NAMES

TYPE	* VALUE	ACTIONS
NT_principal_Name	Example value	

Clear

Add

1 Nazwa

- Wprowadź nazwę profilu SCEP

- Maksymalna długość tekstu to 255
- Wymagane

2

Podstawowa konfiguracja

2.1 Adres dostępowy

- Wprowadź nazwę URL dla serwera SCEP (np. Network Device Enrollment Service)
- Domyślnie obsługiwany jest tylko port 80 (HTTP)
- Przykładowy URL: `http:///certsrv/mscep/mscep.dll`
- Maksymalna długość tekstu to 255
- Wymagane

2.2 ID CA

- Wprowadź nazwę profilu dla serwerów SCEP (np. Network Device Enrollment Service), które obsługują profile nazwane.
- Maksymalna długość tekstu to 255

2.3 Podmiot

- Dostępne zmienne globalne
- Wymagane

2.4 Algorytm szyfrowania

- Typ algorytmu szyfrowania. Określa, jak mocne będzie zabezpieczenie.
- Jedno z:
 - DES
 - DES3
 - AES128
 - AES192
 - AES256
- Wymagane

2.5 Podpis szyfrowania

- Typ podpisu szyfrowania. Określa, jak mocne będzie zabezpieczenie.
- Jedno z:
 - SHA1
 - SHA256
 - SHA384
 - SHA512
- Wymagane

2.6 Długość klucza

- Długość klucza. Określa, jak mocne będzie zabezpieczenie
- Jedno z:
 - 1024
 - 2048
 - 3072
 - 4096
- Wymagane

2.7 Odcisk

- Wprowadź odcisk CA wydającego certyfikat główny na serwerze SCEP (np. Network Device Enrollment Service)
- Maksymalna długość tekstu to 500
- Wymagane

2.8 Hasło

- Wprowadź 'enrollment static password' wygenerowane podczas wdrażania serwera SCEP
- Obsługiwane jest tylko statyczne hasło
- Wartość powinna być 32-znakowym ciągiem znaków alfanumerycznych
- Maksymalna długość tekstu to 255
- Wymagane

2.9 Szyfrowanie klucza

- Jeśli zaznaczone, użyj jako szyfrowanie klucza
- Użyj, gdy nadawca i odbiorca klucza publicznego muszą wygenerować klucz bez użycia szyfrowania

2.10 Podpis cyfrowy

- Jeśli zaznaczone, użyj jako podpis cyfrowy
- Specyficzny typ podpisu, który jest wspierany przez cyfrowy certyfikat. Zapewnia dowód Twojej tożsamości

3 Nazwy alternatywne

3.1 Typ

- Jedno z:
 - Distinguished_Name
 - NT_principal_Name
 - RFC822_Name
 - DNS_Name
- Wymagane

3.2 Wartość

- Dostępne zmienne globalne
- Wymagane

3.3 Usuń

- Usuwa dodaną nazwę alternatywną

3.4 Wyczyść

- Usuwa wszystkie dodane nazwy alternatywne z listy

3.5 Dodaj

- Dodaje nazwę alternatywną do listy

Urządzenie współdzielone

Zaktualizowano: 3 cze 2026

BETA

Profil Urządzenie współdzielone umożliwia zmianę użytkowników na urządzeniach bez ingerencji administratora. Użytkownicy urządzenia mogą używać danych lokalnych lub domenowych do autoryzacji i weryfikacji.

Kompatybilność:

- Android Enterprise Device Owner
-

* Name:
Example

☐ Login on device ⓘ

☒ Force login

* Login type:
Local ▼

System message:
Example message
(15 / 255 chars)



Sign in

Example message

Username

Password ⓘ

Login

☐ Logout from device ⓘ Coming soon

1 Nazwa

- Wprowadź nazwę profilu urządzenia współdzielonego
- Maksymalna długość tekstu to 255
- Wymagane

2 Logowanie na urządzeniu

- Skonfiguruj sposób logowania na urządzeniu

3 Wymuś logowanie

- Jeśli zaznaczone, użytkownik musi się zalogować, aby korzystać z urządzenia

4 Typ logowania

- Dostępne opcje:
 - Lokalnie
 - Domenowo
- Wymagane

5 Wiadomość systemowa

- Wpisz tekst wiadomości, która będzie wyświetlona na widoku logowania
- Maksymalna długość to 255

6 Podgląd

- Podgląd skonfigurowanego profilu na urządzeniu

7 Wylogowanie z urządzenia

Wkrótce dostępne

VPN

Zaktualizowano: 3 cze 2026

Profil VPN określa sposób łączenia się z lokalną siecią firmową.

Kompatybilność:

- iOS
- macOS

* Name:

Example

TYPE

☐ Proget IPsec

☐ IPsec

☐ IKEv2

☐ L2TP

☐ Custom SSL

1 Nazwa

- Nazwa profilu VPN
- Maksymalna długość tekstu to 255
- Wymagane

2 Proget IPsec

3 IPsec

4 IKEv2

5

L2tp

6

Custom SSL

Proget IPsec

Zaktualizowano: 3 gru 2024

Proget IPsec VPN to niestandardowy protokół składający się z zestawu standardów używanych do ustanowienia połączenia VPN.

GENERAL

Automatic disconnect: ⓘ

0

Wi-Fi exclusions: ⓘ

Add

VPN Requests (Never Connect):

Add

VPN Requests (Connect if needed):

Add

PROXY

Proxy configuration:

None

URL of the proxy auto configuration:

Name or IP address of the proxy server:

Proxy server port:

User: ⓘ

Password: ⓘ

1.1 Rozłącz automatycznie

- Połączenie VPN zostanie automatycznie rozłączone po określonym okresie nieaktywności
- Minimalna wartość to 0
- Maksymalna wartość to 1800
- Jeśli wybrana wartość to 0, to 'Automatyczne rozłączanie' będzie wyłączone

1.2 Wykluczenia Wi-Fi

- Automatyczne rozłączanie po połączeniu z określonym Wi-Fi

1.3 Żądania VPN (Nigdy nie łącz)

- Pole określa nazwę domeny lub adres URL. Określone domeny nie będą wywoływać połączenia VPN ani nie będą dostępne przez istniejące połączenie VPN.

1.4 Żądania VPN (Połącz gdy potrzeba)

- Pole określa nazwę domeny lub adres URL. Wywołanie adresu z domeną określoną w tym polu spowoduje próbę nawiązania połączenia VPN, jeśli rozwiązanie nazwy domeny się powiedzie. Obsługiwane są w pełni kwalifikowane nazwy domen. Obsługiwany jest prefiks z symbolem '*' (wildcard).

2 Proxy IPsec Proget

2.1 Konfiguracja proxy

- Jedno z:
 - Automatyczne
 - Ręczne
- Serwery proxy działają jako przekaźniki między witryną, którą odwiedzasz, a Twoim urządzeniem

2.2 Adres URL automatycznej konfiguracji proxy

- Wpisz URL, przez który cały ruch sieciowy będzie przekierowany
- Wymagane, jeśli wybrano 'Konfiguracja proxy: Automatyczna'

2.3 Nazwa lub adres IP serwera proxy

- Wpisz adres IP lub nazwę hosta serwera VPN
- Wymagane, jeśli wybrano 'Konfiguracja proxy: Ręczna'

2.4 Port serwera proxy

- Wpisz numer portu, który jest częścią informacji adresowych używanych do identyfikacji odbiorców i nadawców wiadomości sieciowych
- Minimalna wartość to 0
- Maksymalna wartość to 65535
- Dostępne, jeśli wybrano 'Konfiguracja proxy: Ręczna'

2.5 Użytkownik

- Wpisz nazwę konta użytkownika do autoryzacji proxy
- Dostępne, jeśli wybrano 'Konfiguracja proxy: Ręczna'

2.6 **Hasło**

- Wpisz hasło użytkownika do autoryzacji proxy
- Dostępne, jeśli wybrano 'Konfiguracja proxy: Ręczna'

IPsec

Zaktualizowano: 3 gru 2024

IPsec VPN to protokół składający się z zestawu standardów używanych do nawiązywania połączenia VPN.

GENERAL

* Server: ⓘ

Example server

User: ⓘ

Password: ⓘ

* Authorization method:

Shared Secret / Group Name

* Shared Secret: ⓘ

Group Name: ⓘ

☐ Ask for password ⓘ

☐ Mixed authentication ⓘ

PROXY

Proxy configuration:

None

URL of the proxy auto configuration:

Name or IP address of the proxy server:

Proxy server port:

User: ⓘ

Password: ⓘ

1.1 Serwer

- Wpisz nazwę lub adres IP serwera VPN
- Wymagane

1.2 Użytkownik

- Wpisz konto użytkownika do autoryzacji połączenia

1.3 Hasło

- Wpisz hasło użytkownika do autoryzacji połączenia

1.4 Metoda autoryzacji

- Metoda autoryzacji
- Nie można zmienić

1.5 Shared Secret

- Wpisz wspólne hasło dla połączenia VPN
- Wymagane

1.6 Hasło grupy

- Wpisz identyfikator grupy dla autoryzacji połączenia

1.7 Pytaj o hasło

- Jeśli zaznaczono, użytkownik będzie proszony o hasło na urządzeniu

1.8 Uwierzytelnianie mieszane

- Autoryzuj połączenie za pomocą hasła, nazwy i certyfikatu serwera

2 Proxy IPsec

2.1 Konfiguracja proxy

- Jedno z:
 - Automatyczna
 - Ręczna
- Serwery proxy działają jako przekaźniki między witryną, którą odwiedzasz, a Twoim urządzeniem

2.2 Adres URL automatycznej konfiguracji proxy

- Wpisz URL, przez który cały ruch przeglądarki będzie przekierowany
- Wymagane jeśli wybrano 'Konfiguracja proxy: Automatyczna'

2.3 Nazwa lub adres IP serwera proxy

- Wpisz adres IP lub nazwę hosta serwera VPN
- Wymagane jeśli wybrano 'Konfiguracja proxy: Ręczna'

2.4 Port serwera proxy

- Wpisz numer portu, który jest częścią informacji adresowych używanych do identyfikacji odbiorców i nadawców wiadomości sieciowych
- Minimalna wartość to 0
- Maksymalna wartość to 65535
- Dostępne jeśli wybrano 'Konfiguracja proxy: Ręczna'

2.5 Użytkownik

- Wpisz nazwę konta użytkownika do autoryzacji proxy
- Dostępne jeśli wybrano 'Konfiguracja proxy: Ręczna'

2.6 Hasło

- Wpisz hasło użytkownika do autoryzacji Proxy
- Dostępne jeśli wybrano 'Konfiguracja proxy: Ręczna'

IKEv2

Zaktualizowano: 3 gru 2024

Internet Key Exchange version 2 (IKEv2) to protokół tunelowania oparty na IPsec, który ustanawia bezpieczną komunikację VPN między urządzeniami VPN oraz definiuje procesy negocjacji i uwierzytelniania dla skojarzeń zabezpieczeń IPsec (SA).

GENERAL * Address: Example address ☐ Disable MOBIKE Dead Peer Detection Rate: None ☐ Disable redirect ☐ Enable certificate revocation check ☐ Enable fallback ☐ Enable PFS TLS minimum version: 1.0 TLS maximum version: 1.0 * Identifier: Example identifier * NAT Keepalive interval: 20 ☐ Enable NAT Keepalive offload * Remote identifier: Example remote identifier ☐ Use configuration attribute internal IP subnet ☐ Per App VPN	CHILD SA PARAMS Diffie-Hellman group: 1 Encryption algorithm: DES Integrity algorithm: SHA2-256 Life time in minutes: 10 IKE SA PARAMS Diffie-Hellman group: 1 Encryption algorithm: DES Integrity algorithm: SHA2-256 Life time in minutes: 10
AUTHORIZATION TYPE ☒ Certificate Certificate type: ECDSA512 * Certificate: Certificate * Certificate profile: certificateVpn SCEP profile: Select Server certificate common name: Server certificate issuer common name: ☐ Extended auth enabled Extended auth type: Select User: Password: ☐ Shared secret Shared Secret: ☐ Extended auth enabled Extended auth type: Select User: Password: Certificate: Select Certificate profile: Select SCEP profile: Select ☐ None ☐ Extended auth enabled Extended auth type: Select User: Password: Certificate: Select Certificate profile: Select SCEP profile: Select	
PROXY Proxy configuration: None URL of the proxy auto configuration: Name or IP address of the proxy server: Proxy server port: User: Password:	

1 Ogólne IKEV2

1.1 Adres

- Wpisz adres URL
- Wymagane

1.2 Wyłącz MOBIKE

- Jeśli zaznaczone, MOBIKE zostanie wyłączone
- MOBIKE pozwala pozostać połączonym z VPN nawet po zmianie sieci przez użytkownika

1.3 Poziom Dead Peer Detection

- Częstotliwość, z jaką klient IKEv2 będzie uruchamiał algorytm DPD (Dead Peer Detection)
- Jedno z:
 - Brak
 - Niski (co 30 minut)
 - Średni (co 10 minut)
 - Wysoki (co minutę)

1.4 Wyłącz przekierowania

- Jeśli zaznaczone, przekierowania serwera IKEv2 są wyłączone

1.5 Włącz sprawdzanie odwołania certyfikatu

- Jeśli zaznaczone, sprawdzanie unieważnienia certyfikatu serwera IKEv2 jest włączone
- Jeśli zaznaczone, podczas negocjacji IKEv2 sprawdzane jest, czy certyfikat identyfikujący serwer został unieważniony

1.6 Włącz tryb awaryjny

- Jeśli zaznaczone, umożliwia użycie danych komórkowych, gdy połączenie Wi-Fi jest słabe

1.7 Włącz PFS

- Jeśli zaznaczone, włączone jest PFS (Perfect Forward Secrecy)

1.8 Minimalna wersja TLS

- Jedno z:
 - 1.0
 - 1.1
 - 1.2

1.9 Maksymalna wersja TLS

- Jedno z:
 - 1.0
 - 1.1
 - 1.2

1.10 Identyfikator

- Wpisz lokalny identyfikator klienta IKEv2
- Wymagane

1.11 Interwał NAT Keepalive

- Wpisz częstotliwość w sekundach, z jaką brama wysyła pakiety utrzymania sesji NAT do swojego partnera, aby utrzymać sesję NAT i umożliwić partnerowi dostęp do urządzenia
- Minimalna wartość to 20
- Maksymalna wartość to 1400
- Wymagane

1.12 Włącz odciążenie NAT Keepalive

- Jeśli zaznaczone, pakiety utrzymania sesji będą przekazywane do sprzętu, gdy urządzenie jest w stanie uśpienia

1.13 Zdalny identyfikator

- Wpisz zdalny identyfikator klienta IKEv2
- Wymagane

1.14 Użyj wewnętrznych atrybutów podsieci IPv4 / IPv6

- Jeśli zaznaczone, konfiguracje tunelowania rozdzielonego nie będą komunikowane poprzez selektory ruchu podczas negocjacji IKE

1.15 VPN na aplikację

- Jeśli zaznaczone, pozwala na użycie konfiguracji VPN na aplikację

2 Child SA Params

2.1 Grupa Diffie-Hellman

- Grupy Diffie-Hellman określają siłę klucza używanego w procesie wymiany kluczy
- Jedno z:
 - 1
 - 2
 - 5
 - 14
 - 15
 - 16
 - 17
 - 18
 - 19
 - 20
 - 21
 - 31

2.2 Algorytm szyfrujący

- Typ algorytmu szyfrowania. Określa siłę bezpieczeństwa
- Jedno z:
 - DES
 - 3DES
 - AES-128
 - AES-256
 - AES-128-GCM
 - AES-256-GCM
 - ChaCha20Poly1305

2.3 Algorytm integralności

- Typ algorytmu integralności. Definiuje, jak silne będzie zabezpieczenie
- Jedno z:
 - SHA1-96
 - SHA1-160
 - SHA2-256
 - SHA2-384
 - SHA2-512

2.4 Żywotność

- Czas trwania żywotności Security Association
- Minimalna wartość to 10
- Maksymalna wartość to 1440

3 IKE SA Params

3.1 Grupa Diffie-Hellman

- Grupy Diffie-Hellman określają siłę klucza użytego w procesie wymiany kluczy
- Jedno z:
 - 1
 - 2
 - 5
 - 14
 - 15
 - 16
 - 17
 - 18
 - 19
 - 20
 - 21
 - 31

3.2 Algorytm szyfrujący

- Typ algorytmu szyfrowania. Definiuje, jak silne będzie zabezpieczenie
- Jedno z:
 - DES
 - 3DES
 - 3DES-128ES
 - AES-256
 - AES-128-GCM
 - AES-256-GCM
 - ChaCha20Poly1305

3.3 Algorytm integralności

- Typ algorytmu integralności. Definiuje, jak silne będzie zabezpieczenie
- Jedno z:
 - SHA1-96
 - SHA1-160
 - SHA2-256
 - SHA2-384
 - SHA2-512

3.4 Żywotność

- Czas trwania żywotności SA (Security Association)
- Minimalna wartość to 10
- Maksymalna wartość to 1440

4 Typ autoryzacji - Certyfikat

4.1 Typ certyfikatu

- Jedno z:
 - RSA
 - ECDSA256
 - ECDSA384
 - ECDSA512
 - Ed25519

4.2 Certyfikat

- Typ certyfikatu utworzonego w systemie Proget
- Jedno z:
 - Certyfikat
 - SCEP

4.3 Profil certyfikatu

- Nazwa profilu certyfikatu, który będzie używany
- Wymagane, jeśli wybrano 'Certyfikat: Certyfikat'

4.4 Profil SCEP

- Nazwa profilu SCEP, który będzie używany
- Wymagane, jeśli wybrano 'Certyfikat: SCEP'

4.5 Nazwa wspólna certyfikatu

- Wprowadź ciąg zawierający wartość pola Nazwa Wspólna Podmiotu certyfikatu serwera IKEv2

4.6 Nazwa wspólna wydawcy certyfikatu

- Wprowadź ciąg zawierający wartość pola Nazwa Wspólna Podmiotu certyfikatu Autorytetu Certyfikacji, który wydał certyfikat serwera IKEv2.

4.7 Włącz EAP

- Jeśli zaznaczone, pozwala na użycie autoryzacji rozszerzonej

4.8 Typ EAP

- Jedno z:
 - Użytkownik
 - Certyfikat
- Wymagane jeśli zaznaczono 'Włącz EAP'

4.9 Użytkownik

- Wpisz nazwę użytkownika
- Wymagane jeśli wybrano 'Typ EAP: Użytkownik'

4.10 Hasło

- Wpisz hasło użytkownika
- Dostępne jeśli wybrano 'Typ EAP: Użytkownik'

5 Typ autoryzacji - Shared secret

5.1 Shared Secret

- Wpisz wspólne hasło dla połączenia VPN
- Wymagane

5.2 Włącz EAP

- Jeśli zaznaczono, umożliwia użycie EAP

5.3 Typ EAP

- Jedno z:
 - Użytkownik
 - Certyfikat
- Wymagane jeśli zaznaczono 'Włącz EAP'

5.4 Użytkownik

- Wpisz nazwę użytkownika
- Wymagane jeśli wybrano 'Typ EAP: Użytkownik'

5.5 Hasło

- Wpisz hasło użytkownika
- Dostępne jeśli, wybrano 'Typ EAP: Użytkownik'

5.6 Certyfikat

- Jedno z:
 - Certyfikat
 - SCEP
- Wymagane jeśli wybrano 'Typ EAP: Certyfikat'

5.7 Profil certyfikatu

- Nazwa profilu certyfikatu, który będzie używany
- Wymagane jeśli wybrano 'Certyfikat: Certyfikat'

5.8 Profil SCEP

- Nazwa profilu SCEP, który będzie używany
- Wymagane jeśli wybrano 'Certyfikat: SCEP'

6 Typ autoryzacji - Brak

6.1 Włącz EAP

- Jeśli zaznaczono, umożliwia użycie EAP

6.2 Typ EAP

- Jedno z:
 - Użytkownik
 - Certyfikat
- Wymagane jeśli zaznaczono 'Włącz EAP'

6.3 Użytkownik

- Wpisz nazwę użytkownika
- Wymagane jeśli wybrano 'Typ EAP: Użytkownik'

6.4 Hasło

- Wpisz hasło użytkownika
- Dostępne jeśli, wybrano 'Typ EAP: Użytkownik'

6.5 Certyfikat

- Jedno z:
 - Certyfikat
 - SCEP
- Wymagane jeśli wybrano 'Typ EAP: Certyfikat'

6.6 Profil certyfikatu

- Wybierz nazwę profilu certyfikatu, który będzie używany
- Wymagane jeśli wybrano 'Certyfikat: Certyfikat'

6.7 Profil SCEP

- Wybierz nazwę profilu SCEP, który będzie używany
- Wymagane jeśli wybrano 'Certyfikat: SCEP'

7 IKEV2 Proxy

7.1 Konfiguracja proxy

- Jedno z:
 - Automatyczna
 - Ręczna
- Serwery proxy działają jako przekaźniki między witryną, którą odwiedzasz, a Twoim urządzeniem

7.2 Adres URL automatycznej konfiguracji proxy

- Wpisz URL, przez który cały ruch przeglądarki będzie przekierowany
- Wymagane jeśli wybrano 'Konfiguracja proxy: Automatyczna'

7.3 Nazwa lub adres IP serwera proxy

- Wpisz adres IP lub nazwę hosta serwera VPN
- Wymagane jeśli wybrano 'Konfiguracja proxy: Ręczna'

7.4 Port serwera proxy

- Wpisz numer portu, który jest częścią informacji adresowych używanych do identyfikacji odbiorców i nadawców wiadomości sieciowych
- Minimalna wartość to 0
- Maksymalna wartość to 65535
- Dostępne jeśli wybrano 'Konfiguracja proxy: Ręczna'

7.5 Użytkownik

- Wpisz nazwę konta użytkownika do autoryzacji proxy
- Dostępne jeśli wybrano 'Konfiguracja proxy: Ręczna'

7.6 Hasło

- Wpisz hasło użytkownika do autoryzacji Proxy
- Dostępne jeśli wybrano 'Konfiguracja proxy: Ręczna'

L2TP

Zaktualizowano: 3 gru 2024

Połączenia L2TP (Layer 2 Tunneling Protocol) zapewniają ekonomiczny dostęp dla użytkowników zdalnych, umożliwiając systemom sieci korporacyjnej zarządzanie adresami IP przypisanymi do użytkowników zdalnych.

GENERAL

* Address:

Example address

* User:

Example user

Password:

* Shared Secret:

* Disconnect on idle timer (in seconds):

1

☐ Disconnect on idle

☐ Send all traffic through VPN

PROXY

Proxy configuration:

None

URL of the proxy auto configuration:

Name or IP address of the proxy server:

Proxy server port:

User:

Password:

1.1 Adres

- Adres IP lub nazwa hosta serwera VPN
- Wymagane

1.2 Użytkownik

- Wpisz nazwę użytkownika
- Wymagane

1.3 Hasło

- Wpisz hasło użytkownika

1.4 Shared Secret

- Wpisz wspólne hasło dla połączenia VPN
- Wymagane

1.5 Czas opóźnienia rozłączenia (w sekundach)

- Określa długość czasu oczekiwania przed rozłączeniem połączenia na żądanie
- Minimalna wartość to 1
- Maksymalna wartość to 9007199254740991
- Wymagane

1.6 Opóźnienie rozłączenia

- Jeśli zaznaczono, rozłącza po okresie bezczynności połączenia na żądanie

1.7 Wyślij cały ruch przez VPN

- Jeśli zaznaczono, cały ruch sieciowy będzie przesyłany przez VPN

2 Proxy L2TP

2.1 Konfiguracja proxy

- Jedno z:
 - Automatyczna
 - Ręczna
- Serwery proxy działają jako przekaźniki między witryną, którą odwiedzasz, a Twoim urządzeniem

2.2 Adres URL automatycznej konfiguracji proxy

- Wpisz URL, przez który cały ruch przeglądarki będzie przekierowany
- Wymagane jeśli wybrano 'Konfiguracja proxy: Automatyczna'

2.3 Nazwa lub adres IP auto serwera proxy

- Wpisz adres IP lub nazwę hosta serwera VPN
- Wymagane jeśli wybrano 'Konfiguracja proxy: Ręczne'

2.4 Port serwera proxy

- Wpisz numer portu, który jest częścią informacji adresowych używanych do identyfikacji odbiorców i nadawców wiadomości sieciowych
- Minimalna wartość to 0
- Maksymalna wartość to 65535
- Dostępne jeśli wybrano 'Konfiguracja proxy: Ręczna'

2.5 Użytkownik

- Wpisz nazwę konta użytkownika do autoryzacji proxy
- Dostępne jeśli wybrano 'Konfiguracja proxy: Ręczna'

2.6 **Hasło**

- Wpisz hasło użytkownika do autoryzacji Proxy
- Dostępne jeśli wybrano 'Konfiguracja proxy: Ręczna'

Custom SSL

Zaktualizowano: 3 gru 2024

Secure Sockets Layer VPN (SSL VPN) umożliwia indywidualnym użytkownikom dostęp do sieci organizacji, aplikacji klient-serwer oraz wewnętrznych narzędzi sieciowych i katalogów bez potrzeby korzystania ze specjalistycznego oprogramowania.

* Identifier: Example Identifier * Server: Example server User: Provider bundle ID: Provider designated requirement:	Provider type: App Proxy Disconnect on idle timer (in seconds): 1 ☐ Per App VPN ☐ VPN on demand ☐ Send all traffic through VPN ☐ Exclude local network ☐ Disconnect on idle												
CUSTOM DATA Selected: 0 Deselect all <table><thead><tr><th>☐</th><th>* KEY</th><th>VALUE</th></tr></thead><tbody><tr><td>☐</td><td>Key</td><td>Value</td></tr></tbody></table> Results: 1 ⏪ ⏴ 1 ⏵ ⏩ Add ON DEMAND RULES Selected: 0 Deselect all <table><thead><tr><th>☐</th><th>* DOMAIN</th><th>* ACTION</th></tr></thead><tbody><tr><td>☐</td><td>Domain</td><td>Always</td></tr></tbody></table> Results: 1 ⏪ ⏴ 1 ⏵ ⏩ Add	☐	* KEY	VALUE	☐	Key	Value	☐	* DOMAIN	* ACTION	☐	Domain	Always	
☐	* KEY	VALUE											
☐	Key	Value											
☐	* DOMAIN	* ACTION											
☐	Domain	Always											
AUTHORIZATION TYPE Certificate * Certificate profile: certificateVpn	Password:												
PROXY Proxy configuration: None URL of the proxy auto configuration: Name or IP address of the proxy server: User:	Proxy server port: Password:												

1.1 Identyfikator

- Identyfikator pakietu aplikacji. Jeśli konfiguracja jest skierowana na rozwiązanie VPN, które wykorzystuje dostawcę NetworkExtension, to pole zawiera identyfikator pakietu aplikacji, która zawiera dostawcę. Skontaktuj się z dostawcą rozwiązania VPN w celu uzyskania wartości identyfikatora.
- Maksymalna długość tekstu to 255
- Wymagane

1.2 Serwer

- Wprowadź adres URL serwera
- Maksymalna długość tekstu to 255
- Wymagane

1.3 Użytkownik

- Wprowadź nazwę użytkownika
- Maksymalna długość tekstu to 255

1.4 Identyfikator pakietu dostawcy

- Wprowadź identyfikator pakietu dla dostawcy VPN
- Maksymalna długość tekstu to 255

1.5 Wymagania wyznaczone przez dostawcę

- Użyj tego pola tylko, gdy dostawca VPN jest zaimplementowany jako rozszerzenie systemowe
- Maksymalna długość tekstu to 255
- Wymagane, jeśli dostawca VPN jest zaimplementowany jako rozszerzenie systemowe

2 Opcje CustomSSL

2.1 Rodzaj dostawcy

- Typ usługi VPN
- Jedno z:
 - Proxy aplikacji
 - Tunel pakietów
- Jeśli wybrano 'Proxy aplikacji', usługa będzie tunelować ruch na poziomie aplikacji
- Jeśli wybrano 'Tunel pakietów', usługa będzie tunelować ruch na poziomie IP

2.2 Czas opóźnienia rozłączenia

- Określa jak długo tunel jest aktywny po ostatniej sesji
- Minimalna wartość to 1
- Maksymalna wartość to 9007199254740991
- Wymagane

2.3 VPN dla aplikacji

- Jeśli zaznaczone, konfiguracja VPN jest dostępna tylko dla aplikacji

2.4 VPN na żądanie

- Jeśli zaznaczone, pozwala systemowi na automatyczne rozpoczęcie lub zatrzymanie połączenia VPN na podstawie różnych kryteriów

2.5 Wyślij cały ruch przez VPN

- Jeśli zaznaczone, cały ruch sieciowy zostanie przekierowany przez VPN

2.6 Wyklucz sieć lokalną

- Jeśli zaznaczone, kieruje cały ruch lokalnej sieci poza VPN

2.7 Opóźnienie rozłączania

- Jeśli zaznaczone, odłącza po bezczynności połączenia na żądanie

3 Dane niestandardowe

3.1 Usuń

- Usuwa wybrany klucz

3.2 Klucz

- Specyficzne ustawienia par klucz-wartość
- Słownik konfiguracji specyficznej dla danego rozwiązania VPN strony trzeciej
- Odniesienie do dokumentacji rozwiązania VPN strony trzeciej, aby dowiedzieć się o słowniku konfiguracji
- Odniesienie do bazy wiedzy Proget, aby dowiedzieć się o słowniku konfiguracji OpenVPN

3.3 Wartość

- Specyficzne ustawienia par klucz-wartość
- Słownik konfiguracji specyficznej dla danego rozwiązania VPN strony trzeciej
- Odniesienie do dokumentacji rozwiązania VPN strony trzeciej, aby dowiedzieć się o słowniku konfiguracji
- Odniesienie do bazy wiedzy Proget, aby dowiedzieć się o słowniku konfiguracji OpenVPN

3.4 Dodaj

- Dodaj nowy klucz

4 Reguły na żądanie

4.1 Usuń

- Usuwa wybraną domenę

4.2 Domena

- Wprowadź nazwę domeny
- Wymagane, jeśli dodane są reguły na żądanie

4.3 Akcja

- Jedno z:
 - Nigdy
 - Gdy potrzeba
 - Zawsze
- Jeśli wybrano 'Nigdy', gdy nazwa hosta kończy się na jedną z tych nazw domeny, VPN nie jest uruchamiany automatycznie. Jest to używane do wykluczenia subdomeny w ramach zawartej domeny.
- Jeśli wybrano 'Gdy potrzeba', gdy nazwa hosta kończy się na jedną z tych nazw domeny i zapytanie DNS dla tej nazwy domeny zawiedzie, VPN jest uruchamiany automatycznie
- Jeśli wybrano 'Zawsze', domeny powiązane są traktowane tak, jakby były związane z kluczem 'Jeśli potrzebne'

4.4 Dodaj

- Dodaj nową domenę

5 Typ autoryzacji

5.1 Typ

- Metoda uwierzytelniania do użycia
- Jedno z:
 - Certyfikat
 - Hasło

5.2 Profil certyfikatu

- Wybierz profil certyfikatu, który będzie używany
- Wymagane, jeśli wybrano 'Typ: Certyfikat'

5.3 Hasło

- Hasło wymagane do autoryzacji
- Dostępne jeśli wybrano 'Typ: Hasło'

6 Proxy CustomSSL

6.1 Konfiguracja Proxy

- Jedno z:
 - Automatyczna
 - Ręczna
- Serwery proxy działają jako pośredniki między odwiedzaną stroną internetową a urządzeniem

6.2 Adres URL konfiguracji automatycznej proxy

- Wprowadź URL, przez który cały ruch przeglądarki zostanie przekierowany
- Wymagane, jeśli wybrano 'Konfiguracja Proxy: Automatyczna'

6.3 Nazwa lub adres IP serwera proxy

- Wprowadź adres IP lub nazwę hosta serwera VPN
- Wymagane, jeśli wybrano 'Konfiguracja Proxy: Ręczna'

6.4 Port serwera proxy

- Wprowadź numer portu, który jest częścią informacji adresowej używanej do identyfikacji odbiorców i nadawców wiadomości sieciowych
- Minimalna wartość to 0
- Maksymalna wartość to 65535
- Dostępne, jeśli wybrano 'Konfiguracja Proxy: Ręczna'

6.5 Użytkownik

- Wprowadź nazwę konta użytkownika dla uwierzytelniania proxy
- Dostępne, jeśli wybrano 'Konfiguracja Proxy: Ręczna'

6.6 **Hasło**

- Wprowadź hasło użytkownika dla uwierzytelnienia proxy
- Dostępne, jeśli wybrano 'Konfiguracja Proxy: Ręczna'

Tapeta

Zaktualizowano: 3 cze 2026

Profil Tapeta pozwala spersonalizować obraz ekranu głównego oraz ekranu blokady na urządzeniu z systemem Android oraz iOS z włączonym trybem nadzorowanym.

Kompatybilność:

- Android
 - Android Enterprise Device Owner
 - iOS (tryb nadzorowany)
-

* Name:

Example

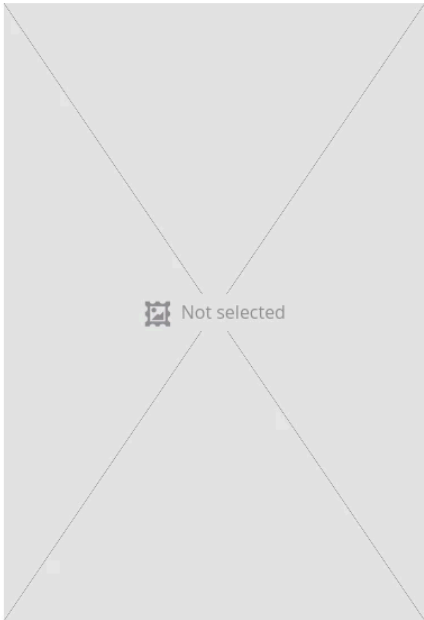
☒ Scale image to device screen size ⓘ

HOME SCREEN WALLPAPER



Select file wallpaper.png - 1.56 KiB (1.60 KB)

LOCK SCREEN WALLPAPER



Select file

Back Submit

1 Nazwa

- Wprowadź nazwę profilu tapety
- Maksymalna długość tekstu to 255
- Wymagane

2 Skaluj obraz do wielkości ekranu urządzenia

- Dostępne tylko na urządzeniach z Androidem

3 Tapeta ekranu głównego

- Podgląd tapety na głównym ekranie urządzenia

4 Tapeta ekranu blokady

- Podgląd tapety na ekranie blokady urządzenia

5 Wybierz plik z tapetą ekranu głównego

- Dozwolone typy plików: png
- Maksymalny rozmiar pliku: 10MB
- Wymagane, jeśli 'Tapeta ekranu blokady' jest pusta

6 Wybierz plik z tapetą ekranu blokady

- Dozwolony typ pliku: png
- Maksymalny rozmiar pliku: 10MB
- Wymagane, jeśli 'Tapeta ekranu głównego' jest pusta

Wi-Fi

Zaktualizowano: 3 cze 2026

Profil Wi-Fi określa zaufane sieci bezprzewodowe, udostępnione w środowisku firmowym, sposób łączenia się i bezpiecznej autoryzacji.

Kompatybilność:

- Android (do androida 9)
- Android Enterprise Device Owner
- Android Enterprise Profile Owner
- iOS
- macOS

* Name:

Example

CONFIGURATION

* SSID:

Wi-Fi Example SSID

☐ Hidden network

☐ Auto Join

☐ Set static MAC address ⓘ

Security type:

Enterprise ▼

Preshared key:

👁

ENTERPRISE

Authentication protocol:

EAP-PEAP ▼

Domain: ⓘ

Example domain

CA:

Do not validate ▼

Access certificate:

Certificate ▼

Certificate profile:

Select ▼

SCEP profile:

Select ▼

* Username:

Example username

* Password:

👁

☐ Use Per-Connection password

Outer identity:

Inner authentication:

None ▼

☐ Use Protected Access Credential (PAC)

☐ Provision PAC

☐ Provision PAC anonymously

1 Nazwa

- Wpisz nazwę profilu Wi-Fi
- Maksymalna długość tekstu to 255

- Wymagane

2

Dane Wi-Fi

2.1 SSID

- Wpisz nazwę identyfikującą sieć bezprzewodową
- Wymagane

2.2 Ukryta sieć

- Wymagane, jeśli dla sieci, dla której przygotowujemy konfigurację, ukryto SSID

2.3 Auto Join

- Wymagane, jeśli urządzenie potrzebuje domyślnej sieci

2.4 Ustaw stały adres MAC

- Wymagane, jeśli urządzenie potrzebuje nierandomizowanego adresu MAC

2.5 Typ zabezpieczeń

- Jeden z:
 - Brak
 - Personal WPA/WPA2
 - Personal WPA/WPA3
 - Enterprise
- Jeśli wybrano 'Brak', sieć będzie bez zabezpieczeń
- Jeśli wybrano 'Personal WPA/WPA2' lub 'Personal WPA/WPA3', zarządzanie autentykacją użytkownika odbywa się poprzez WPA klucz współdzielony
- Jeśli wybrano 'Enterprise', zarządzanie autentykacją użytkownika odbywa się poprzez protokół zdalnej autentykacji

2.6 Klucz współdzielony

- Wpisz współdzielony klucz, aby uwierzytelnić się w Wi-Fi

- Dostępne, jeśli wybrano "Typ zabezpieczenia: Personal WPA/WPA2", lub 'Personal WPA/WPA3'

3 Wi-Fi Enterprise - 1

3.1 Protokół uwierzytelniania

- Jeden z:
 - EAP-TLS
 - EAP-TTLS
 - EAP-PEAP
 - EAP-FAST

3.2 Domena

- Można podać wiele domen, oddzielając je średnikami (np. example.org;example.com)

3.3 CA

- Wybierz certyfikat stworzony w Proget, który będzie wymagany do uwierzytelnienia w Wi-Fi

3.4 Certyfikat dostępowy

- Jeden z:
 - Certyfikat
 - Profil SCEP
- Dostępne, jeśli wybrano "Protokół uwierzytelniania: EAP-TLS"

3.5 Profil certyfikatu

- Wybierz profil SCEP stworzony w Proget, który będzie wymagany do uwierzytelnienia w Wi-Fi
- Dostępne, jeśli wybrano "Protokół uwierzytelniania: EAP-TLS"
- Dostępne, jeśli wybrano "Certyfikat dostępu: Certyfikat"

3.6 Profil SCEP

- Wybierz profil SCEP stworzony w Proget, który będzie wymagany do uwierzytelnienia w Wi-Fi
- Dostępne, jeśli wybrano "Protokół uwierzytelniania: EAP-TLS"

- Dostępne, jeśli wybrano "Certyfikat dostępu: SCEP"

4 Wi-Fi Enterprise - 2

4.1 Użytkownik

- Maksymalna długość tekstu to 64
- Wymagane

4.2 Hasło

- Dostępne, jeśli wybrano "Protokół uwierzytelniania: EAP-TTLS / EAP-PEAP / EAP-FAST"
- Maksymalna długość tekstu to 64
- Wymagane

4.3 Żądaj hasła przy połączeniu

- Jeśli zaznaczone, wymagane jest podanie hasła przy połączeniu
- Dostępne, jeśli wybrano "Protokół uwierzytelniania: EAP-TTLS / EAP-PEAP / EAP-FAST"

4.4 Tożsamość widoczna zewnątrz

- Dostępne, jeśli wybrano "Protokół uwierzytelniania: EAP-TTLS / EAP-PEAP / EAP-FAST"
- Maksymalna długość tekstu to 256

4.5 Uwierzytelnienie wewnętrzne

- Dostępne, jeśli wybrano protokół uwierzytelniania EAP-TTLS
- Jeden z:
 - Brak
 - PAP
 - CHAP
 - MSCHAP
 - MSCHAPV2
 - GTC
 - EAP

- Dostępne, jeśli wybrano "Protokół uwierzytelniania: EAP-TTLS"

4.6 Używaj Protected Access Credential (PAC)

- Dostępne, jeśli wybrano "Protokół uwierzytelniania: EAP-FAST"

4.7 Zaopatruj PAC

- Dostępne, jeśli wybrano "Protokół uwierzytelniania: EAP-FAST"
- Dostępne, jeśli zaznaczono "Używaj Protected Access Credential (PAC)"

4.8 Zaopatruj PAC anonimowo

- Dostępne, jeśli wybrano "Protokół uwierzytelniania: EAP-FAST"
- Dostępne, jeśli zaznaczono "Używaj Protected Access Credential (PAC)"
- Dostępne, jeśli zaznaczono "Przydziel PAC"

Etykiety

Zaktualizowano: 3 cze 2026

Etykietowanie grup oraz użytkowników umożliwia przypisywanie urządzeń do nich.

Reset filters

Selected: 0 | Deselect all



Add 

☐	NAME	USERS	ROLES	LDAP	ENTR...	GROU...
☐	admin	0	1	0	0	1
☐	user	1	1	0	0	1

Results: 2 | Page limit: 50



1 Filtr

- Użyj filtrów aby wyszukać odpowiednią etykietę

2 Powiązania

- Ta akcja pozwala wyświetlić wszystkie powiązania etykiety

3 Edytuj

- Ta akcja pozwala na edycję wybranej etykiety z listy

4 Usun

- Ta akcja pozwala na usunięcie wybranych etykiet z listy

5 Dodaj etykietę

5.1 Nazwa etykiety

- Ustaw nazwę aby utworzyć nową etykietę
- Wymagane

5.2 Kolor

- Wybierz kolor etykiety
- Wymagane

6 Lista etykiet

- Lista etykiet, które zostały utworzone wraz z liczbą powiązań z określonymi elementami

Logi audytowe

Zaktualizowano: 3 cze 2026

Miejsce przeznaczone do zbierania i przeglądania informacji na temat zdarzeń zachodzących na serwerze.

Audit logs

 Give feedback

Action: Select  

Status: Select  

Date of occurrence: From Select To Select  

Reset filtersBASICPQL

ACTION	STATUS	DATE OF OCCURRENCE 	PERFORMED BY	PERFORMED ON	DETAILS
user.authenticate	Success	2025-07-08 14:19:12	Ironman Ironman (...)	Ironman Ironman (...)	User authentication success. Authentication (l...

1

Filtr

- Użyj filtrów aby wyszukać odpowiedni log

2

Lista logów

- Lista logów, które zostały wygenerowane w wyniku określonej akcji w konsoli

Zadania

Zaktualizowano: 3 gru 2024

Zadania wysyłane do urządzeń utworzone przez użytkowników systemu lub przez system.

Action: Select ⌵ 🗑Serial number: Start typing... 🗑IMEI: Start typing... 🗑User: Start typing... 🗑 +

Reset filters

Selected: 0 | Deselect all 🔄 🗑

☐	SENT DATE ⌵	COMPLETE DATE ⌵	ACTION	CREATED BY	MANUFACTURER	MODEL	USER	STATUS
☐	2024-08-31 14:52:37	2024-08-31 14:52:42	Change password	jdoe	SAMSUNG	SM-A225F	John Doe	Success
☐	2024-08-31 14:52:18	2024-08-31 14:52:25	Send message	jdoe	SAMSUNG	SM-A225F	John Doe	Success
☐	2024-08-31 14:52:03	2024-08-31 14:52:04	Install app 🔗	jdoe	SAMSUNG	SM-A225F	John Doe	Success
☐	2024-08-31 13:56:15	2024-08-31 13:56:15	Policy update 🔗	system	SAMSUNG	SM-A225F	John Doe	Success
☐	2024-08-31 13:56:15	2024-08-31 13:56:15	Refresh device data	system	SAMSUNG	SM-A225F	John Doe	Success

Results: 5 | Page limit: 50 ⌵

⏪ ⏴ 1 ⏵ ⏩

1 Filtry

- Użyj filtrów, aby wyszukać odpowiednie zadania

2 Powtórz zadanie

- Ta akcja pozwala na ponowne uruchomienie wybranych zadań ze statusem Nie wykonano

3 Usuń zadanie

- Ta akcja pozwala na usunięcie wybranych zadań ze statusem utworzony, oczekujący, otrzymany, niepowodzenie i anulowany

4 Lista zadań

- Lista wszystkich zadań wraz z ich parametrami

Serwis

Zaktualizowano: 3 cze 2026

Zakładka Serwis zawiera dane o urządzeniach, które kiedykolwiek zostały aktywowane na danym serwerze, nawet po dezaktywacji, aż do zniszczenia serwera.

IMEI: 352946245353881 XSerial number: R0C7T714K038 XUser: Start typing... XManufacturer: Select X+

Reset filters

Selected: 1Deselect all

MANUFACTURER

MODEL

IMEI

SERIAL NUMBER

USER

FILES

SAMSUNG

SM-G991B

352946245353881
R0C7T714K038

R0C7T714K038

John Doe

example.csv - 169 B X

...

Results: 1 | Page limit: 50

1

1Filtr

- Użyj filtrów, aby wyszukać odpowiednie urządzenie

2Akcje

2.1 Zaktualizuj dane

- Ta akcja pozwala na aktualizację danych wybranego urządzenia

2.2 Ustaw komentarz

- Ta akcja pozwala na ustawienie komentarza dla wybranego urządzenia

2.3 Historia użytkowników urządzenia

- Ta akcja pozwala na wyświetlenie historii użytkowników urządzenia

2.4 Eksportuj informacje

- Ta akcja pozwala na eksport informacji z wybranego urządzenia

2.5 Kody zabezpieczeń

Przestarzała

- Ta akcja wyświetla kody zabezpieczeń dla wybranego urządzenia

2.6 Wyślij pliki

- Ta akcja pozwala na przesłanie plików do kolumny plików wybranego urządzenia

2.7 Pobierz pliki

- Ta akcja pozwala na pobieranie plików z kolumny plików wybranego urządzenia

2.8 Usuń pliki

- Ta akcja pozwala na usunięcie plików z kolumny plików wybranego urządzenia

3 Lista urządzeń

- Lista urządzeń, które kiedykolwiek zostały aktywowane na danym serwerze, nawet po dezaktywacji, aż do zniszczenia serwera

Aktualizacja

Zaktualizowano: 16 lip 2026

W widoku aktualizacji informacji o urządzeniu możesz edytować dane dotyczące danego urządzenia.

Update device information

Device name:

SAMSUNG

Model:

SM-G991B

Serial number:

48562771544028

IMEI:

352096246520961, 352096246520961

User:

John Doe

Invoice No:

Example

Date of purchase:

Select date

Warranty:

Example

Operator:

Example

Agreement expiration date:

Select date

Address:

Example

Comment:

WYŚWIETLAK

B**I****U****S**

3

Insert text here...

(0 / 550 chars)

1 Nazwa urządzenia

- Wyświetla nazwę urządzenia - producent
- To pole nie może być modyfikowane

2 Model

- Wyświetla model urządzenia
- To pole nie może być modyfikowane

3 Numer seryjny

- Wyświetla numer seryjny urządzenia
- To pole nie może być modyfikowane

4 IMEI

- Wyświetla IMEI urządzenia
- To pole nie może być modyfikowane

5 Użytkownik

- Wyświetla aktualnie przypisanego użytkownika

- To pole nie może być modyfikowane

6 Nr faktury

- Wprowadź nr faktury

7 Data zakupu

- Wprowadź datę zakupu

8 Gwarancja

- Wprowadź informacje o gwarancji

9 Operator

- Wprowadź informacje o operatorze

10 Data wygaśnięcia umowy

- Wprowadź datę wygaśnięcia umowy

11 Adres

- Wprowadź adres

12 Komentarz

- Wprowadź wszelkie dodatkowe informacje

Historia serwisu

Zaktualizowano: 28 maj 2026

Historia użytkowników urządzenia zawiera dane o poprzednich użytkownikach danego urządzenia.

Device users history

Selected: 1

Deselect all

☒ USER	REGISTRATION TYPE	REGISTRATION DATE	DEREGISTRATION DATE	LOCATION	PHONE	
☒ John Doe	Android Enterprise Device Owner	2024-01-18 14:14:12	2024-01-18 15:53:33	-	-	...

Results: 1

Page limit: 50

<<

<

1

>

>>

1

Generuj hasło serwisowe

- Generuje hasło serwisowe dla wybranej rejestracji wybranego urządzenia

2

Lista historii użytkowników urządzenia

- Lista historii użytkowników urządzenia z typem rejestracji, datą rejestracji, lokalizacją i telefonem

Hasło serwisowe

Zaktualizowano: 9 cze 2026

NOWOŚĆ

Panel Hasło serwisowe dostępny w zakładce Serwis umożliwia administratorowi wygenerowanie awaryjnego hasła serwisowego dla dowolnego urządzenia. Hasło jest powiązane z konkretnym urządzeniem i ma określony czas ważności (domyślnie 24 godziny, minimalnie 5 minut, maksymalnie 30 dni). Działa nawet gdy urządzenie nie ma połączenia z internetem lub lokalna baza danych jest uszkodzona. Dostępne akcje i ich zachowanie zależą od typu aktywacji urządzenia - niektóre opcje mogą być niedostępne lub działać inaczej na aktywacjach COPE i Android MDM. Po użyciu urządzenie wchodzi w 60-minutowe okno uprzywilejowanego działania, po czym wraca do stanu wymaganego przez polityki. Hasło można wpisać ręcznie lub zeskanować jako kod QR na urządzeniu.



Service password

* Select actions: ⓘ

- ☐ Unblock device
- ☐ Disable Kiosk
- ☐ Remove network restrictions ⓘ
- ☐ Allow developer options
- ☐ Allow deactivation
- ☐ Allow factory reset
- ☐ Emergency Database Reset ⓘ
- ☐ Set Password ⓘ

* Service password expiration date (on device):

2026-05-07 10:23



Time to expire: in about 24 hours

- ☒ Generate QR code
- ☒ Send service password via email

* Email:

example@domain.com

Message language:

English



Cancel

Generate

1 Odblokuj urządzenie

- Jeśli zaznaczone, hasło serwisowe odblokuje urządzenie z trybu Lost Mode
- Zachowanie zależy od typu aktywacji urządzenia

2 Wyłącz Kiosk

- Jeśli zaznaczone, hasło serwisowe wyjdzie z trybu Kiosk na urządzeniu
- Dostępne tylko na aktywacjach obsługujących profil Kiosk

3 Usuń ograniczenia sieciowe

- Jeśli zaznaczone, hasło serwisowe tymczasowo usunie ograniczenia sieciowe nałożone przez polityki związane z siecią na urządzeniu

4 Zezwól na opcje programistyczne

- Jeśli zaznaczone, hasło serwisowe tymczasowo włączy opcje programistyczne na urządzeniu

5 Pozwalaj na dezaktywację

- Jeśli zaznaczone, hasło serwisowe pozwoli użytkownikowi na dezaktywację aplikacji Proget MDM na urządzeniu

6 Pozwalaj na przywrócenie do ustawień fabrycznych

- Jeśli zaznaczone, hasło serwisowe pozwoli użytkownikowi na przywrócenie urządzenia do ustawień fabrycznych

7 Awaryjny reset bazy danych

- Jeśli zaznaczone, hasło serwisowe autoryzuje awaryjny reset bazy danych aplikacji Proget MDM na urządzeniu
- Nie można łączyć z innymi akcjami

8 Ustaw hasło

- Jeśli zaznaczone, hasło serwisowe pozwoli na ustawienie nowego hasła urządzenia w scenariuszu Direct Boot (po restarcie urządzenia)
- Nie można łączyć z innymi akcjami
- Zachowanie zależy od typu aktywacji urządzenia

9 Data wygaśnięcia hasła serwisowego (na urządzeniu)

- Ustaw datę i godzinę, kiedy hasło serwisowe wygaśnie na urządzeniu
- Domyślna ważność to 24 godziny, minimalnie 5 minut, maksymalnie 30 dni

10 Generuj kod QR

- Jeśli zaznaczone, wraz z hasłem serwisowym zostanie wygenerowany kod QR do łatwiejszego zeskanowania na urządzeniu

11 Wyślij hasło serwisowe wiadomością email

- Jeśli zaznaczone, wygenerowane hasło serwisowe zostanie wysłane na podany adres email

12 Email

- Wprowadź adres email, na który zostanie wysłane hasło serwisowe
- Wymagane, jeśli zaznaczono 'Wyślij hasło serwisowe wiadomością email'

13 Język wiadomości

- Wybierz język, w którym zostanie wysłana wiadomość email z hasłem serwisowym

14 Generuj

14.1 Wygenerowane hasło serwisowe dla urządzenia

- Wyświetla wygenerowane hasło serwisowe dla urządzenia
- Hasło można skopiować do schowka za pomocą ikony kopiowania

14.2 Kod QR

- Wyświetla kod QR zawierający hasło serwisowe do zeskanowania na urządzeniu
- Widoczny tylko jeśli zaznaczono 'Generuj kod QR'

Bezpieczeństwo

Zaktualizowano: 3 gru 2024

W tym miejscu znajdziesz tabelę z listą zdarzeń bezpieczeństwa na urządzeniach.

Status: Select

Name: Select

User: Start typing...

Event status: Select

Reset filters

STATUS	NAME	DATE	USER	MANUFACT...	MODEL	DEVICE STA...	EVENT STA...
Safe	Access to Wi-Fi management	2024-08-31 14:33:45	John Doe	SAMSUNG	SM-A225F	Active	Current
Information	Access to device usage data	2024-08-31 14:33:45	John Doe	SAMSUNG	SM-A225F	Active	Current
> Safe	No password on the device	2024-08-31 14:24:49	John Doe	SAMSUNG	SM-A225F	Active	Archival
Safe	Proget Remote installed	2024-08-31 13:57:38	John Doe	SAMSUNG	SM-A225F	Active	Current
Safe	Play Integrity verification status	2024-08-31 13:56:20	John Doe	SAMSUNG	SM-A225F	Active	Current
Safe	Root status	2024-08-31 13:56:11	John Doe	SAMSUNG	SM-A225F	Active	Current

Results: 6 | Page limit: 50

<<

<

1

>

>>

1 Filtry

- Filtr bezpieczeństwa pozwala wyszukiwać informacje według danych, takich jak:
 - Status
 - Nazwa
 - Data
 - Użytkownik
 - Producent
 - Model
 - Status urządzenia
 - Status zdarzenia

2 Lista zdarzeń bezpieczeństwa na urządzeniach

- Lista wszystkich zdarzeń bezpieczeństwa, które wystąpiły na urządzeniu wraz z ich parametrami

Raporty

Zaktualizowano: 3 cze 2026

W tym miejscu można konfigurować i generować raporty zawierające wszystkie ważne informacje o urządzeniach w systemie.

ListConfiguration

Name: Insert text here...

Type: Select

Date: From Select ... To Select date

Reset filters

Selected: 1

Deselect all

Generate

☒	NAME	TYPE	DATE	SIZE	
☒	Example	Custom	2024-09-04 13:10:20	16.73 KiB (17.13 KB)	...

Results: 1

Page limit: 50

1

1 Lista

- Lista wyświetla wszystkie raporty, które wygenerowałeś i które zawierają informacje o urządzeniach

2 Konfiguracja

- Konfiguracja służy do stworzenia własnego raportu ze specyficznymi zmiennymi. Raport może być uruchamiany cyklicznie i być powiązany z listą dystrybucyjną w formie adresów email.

Lista raportów

Zaktualizowano: 16 lip 2026

W tym miejscu można znaleźć listę wygenerowanych raportów zawierających wszystkie ważne informacje o urządzeniach w systemie.

List

Configuration

Name: Insert text here...

Type: Select

Date: From Select ... To Select date

Reset filters

Selected: 1

Deselect all

Download

Delete

Generate

☒ NAME	TYPE	DATE	SIZE	
☒ Example	Custom	2024-09-04 13:10:20	16.73 KiB (17.13 KB)	...

Results: 1

Page limit: 50

<<

<

1

>

>>

1 Filtry

- Filtr raportów umożliwia wyszukiwanie raportów według danych, takich jak:
 - Nazwa
 - Typ
 - Data

2 Pobierz

- Ta akcja umożliwia pobranie jednego lub więcej wygenerowanych raportów

3 Usuń

- Ta akcja umożliwia usunięcie jednego lub więcej wygenerowanych raportów

4 Generuj

- Ta akcja przeniesie Cię do widoku, w którym możesz wygenerować raport swoich urządzeń według własnych preferencji

5 Lista wygenerowanych raportów

- Lista wszystkich wygenerowanych raportów wraz z ich parametrami

Generuj raporty

Zaktualizowano: 3 gru 2024

W tym miejscu można wygenerować raport zawierający wybrane informacje o urządzeniach w systemie.

* Report name:

Example

* Format:

PDF

* Orientation:

Vertical

* Type:

Custom

Groups:

Select

☒ Send report via email

* Add recipient(s):

example@mail.com

Add

* Data generated in the report:

☒ Device ID

☐ Device alias

☐ Device vendor

☒ Device model

☐ Operating system

☐ Language

☐ Serial number

☐ IMEI 1

☐ IMEI 2

☐ Last contact

☐ Last contact (days)

☐ Storage (bytes)

☐ Available storage (bytes)

☐ Activation date

☐ Battery health

1 Nazwa raportu

- Podaj nazwę raportu
- Wymagane

2 Format

- W rozwijanym menu wybierz format pliku
- Dostępne formaty plików:
 - CSV
 - PDF
- Wymagane

3 Orientacja

- W rozwijanym menu wybierz orientację
- Orientacja dostępna tylko przy formacie PDF:
 - Pionowa
 - Pozioma
- Wymagane, jeśli wybrano format PDF

4 Typ

- W rozwijanym menu wybierz typ
- Dostępne typy:
 - Własny
 - Aplikacje Proget na urządzeniach
 - Aplikacje na urządzeniach
 - Aplikacje służbowe przypisane do urządzenia
 - Aplikacje służbowe zainstalowane na urządzeniu
 - Logowanie do Kiosku
 - Lokalizacje urządzeń
 - Nieaktywne urządzenia
 - Ostatni kontakt z urządzeniami
 - Ostatnia lokalizacja urządzeń
 - Status bezpieczeństwa urządzeń
 - Urządzenia użytkowników
 - Urządzenia w systemie
- Wymagane

5 Grupy

- W rozwijanym menu możesz wybrać grupę

6 Wyślij raport wiadomością email

- Jeśli zaznaczone, raport zostanie wysłany wiadomością email
- Aby ta funkcja działała prawidłowo, należy skonfigurować SMTP w zakładce Ustawienia

7 Dodaj odbiorcę(-ów)

- Dodaj adres email odbiorcy(-ów), którym zostanie wysłany raport

8

Dane wygenerowane w raporcie

- Jeśli wybrano typ niestandardowy, będziesz mógł zarządzać tym, jakie informacje o urządzeniu zostaną uwzględnione w wygenerowanym raporcie

Konfiguracja

Zaktualizowano: 16 lip 2026

W tym miejscu można dodać konfigurację raportu. Ustaw cykl wykonywania raportu, określ dane i odbiorców. Raporty będą generowane automatycznie i wysyłane pocztą elektroniczną (wymagany SMTP). Wygenerowane raporty można pobrać z zakładki Raporty.

[List](#) **Configuration**

Configuration is used to create your own report with specific variables. The report can be run cyclically and be linked to a distribution list in the form of email addresses.

Name:

Type: Select

[Reset filters](#)

Selected: 1 | [Deselect all](#)

[Add](#)

☒	NAME	TYPE
☒	Example	Custom

Results: 1 | Page limit: 50

1

1 Filtr konfiguracji

- Filtr pozwala na wyszukiwanie raportów według danych, takich jak:
 - Nazwa
 - Typ

2 Edytuj

- Ta akcja pozwala na edycję wybranej konfiguracji

3 Generuj

- Ta akcja pozwala na wygenerowanie raportu, gdy wybrano konfigurację z listy konfiguracji

4 Usun

- Ta akcja pozwala na usunięcie pojedynczej lub większej liczby konfiguracji z listy

5 Dodaj

- Ta akcja przeniesie Cię do widoku, gdzie możesz skonfigurować własną konfigurację

- Lista wszystkich utworzonych konfiguracji

Dodaj konfiguracje

Zaktualizowano: 3 gru 2024

W tym miejscu można dodać konfigurację raportu. Ustaw cykl wykonywania raportu, określ dane i odbiorcę (odbiorców). Raporty będą generowane automatycznie i wysyłane wiadomością email (wymagany SMTP) lub można je pobrać z zakładki Raporty.

* Name:

Example

REPORTS DATA

* Format:

PDF

* Orientation:

Vertical

* Type:

Custom

Groups:

Select

* Select the data to be included in the report

-

Q

☒ Device ID

☐ Device alias

☒ Device vendor

☒ Device model

☐ Operating system

☐ Language

☐ Serial number

☐ IMEI 1

☐ IMEI 2

☐ Last contact

REPORT SCHEDULER

* Recurrence:

☐ Once a day

Hour:

00:00

Scheduled day(s):

☐ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

☐ Sunday

☒ Interval

* Hour:

00:00

* Interval (in days, 1-30):

1

REPORTS HISTORY

* Automatically delete reports older than
(in days, 1-360):

180

OTHER SETTINGS

☒ Send report via email ⓘ

* Add recipient(s):

example@mail.pl

Add

1 Nazwa

- Podaj nazwę konfiguracji
- Wymagane

2 Dodaj dane

2.1 Format

- W rozwijanym menu wybierz format pliku
- Dostępne formaty plików:
 - CSV
 - PDF
- Wymagane

2.2 Orientacja

- W rozwijanym menu wybierz orientację
- Orientacja dostępna tylko przy formacie PDF:
 - Pionowa
 - Pozioma
- Wymagane przy wybranym formacie PDF

2.3 Typ

- W rozwijanym menu wybierz typ
- Dostępne typy:
 - Własny
 - Aplikacje Proget na urządzeniach
 - Aplikacje na urządzeniach
 - Aplikacje służbowe przypisane do urządzenia
 - Aplikacje służbowe zainstalowane na urządzeniu
 - Logowanie do Kiosku
 - Lokalizacje urządzeń
 - Nieaktywne urządzenia
 - Ostatni kontakt z urządzeniami
 - Ostatnia lokalizacja urządzeń

- Status bezpieczeństwa urządzeń
- Urządzenia użytkowników
- Urządzenia w systemie
- Wymagane

2.4 Grupy

- W rozwijanym menu możesz wybrać grupę

2.5 Wybierz dane, które mają zostać zawarte w raporcie

- Jeśli wybrano typ niestandardowy, będziesz mógł zarządzać jakie informacje o urządzeniu zostaną uwzględnione w generowanym raporcie
- Wymagane

3 Dodaj harmonogram

3.1 Raz dziennie

- Jeśli wybrano, musisz wybrać czas i dni, w których raport będzie generowany

3.2 Interwał czasowy

- Jeśli wybrano, musisz ustawić czas i codzienny cykl generowania raportu

4 Dodaj historię

4.1 Automatycznie usuwaj raporty starsze niż (w dniach, 1-360):

- Wybierz liczbę dni, po których wygenerowane raporty zostaną usunięte
- Wymagane

4.2 Wyślij raport wiadomością email

- Jeśli zaznaczone, raport zostanie wysłany wiadomością email
- Aby ta funkcja działała prawidłowo, należy skonfigurować SMTP w zakładce Ustawienia

4.3 Dodaj odbiorcę(-ów)

- Dodaj adres email odbiorcy(-ów), którym zostanie wysłany raport

Ustawienia

Zaktualizowano: 16 lip 2026



Kontrola dostępu

Ograniczanie dostępu do zarządzania do wybranych adresów sieciowych



Dozwolone karty SIM

Zarządzanie kartami SIM dozwolonymi na urządzeniach



Audyt i logowanie

Rejestrowanie logów audytu działań administracyjnych i urządzeń



Microsoft Entra ID

Zarządzanie połączeniem i synchronizacją z Microsoft Entra ID



Menedżer certyfikatów

Zarządzanie certyfikatami używanymi w profilach i aplikacjach



Connector

Konfiguracja połączenia LDAP z Chmurą Proget



Gateway

Bezpieczna brama szyfrująca ruch do systemów pocztowych



Ogólne

Informacje o serwerze oraz jego konfiguracja



LDAP

Zarządzanie połączeniami LDAP do synchronizacji katalogu



SMTP

Konfiguracja SMTP do wiadomości aktywacyjnych i powiadomień



Role

Konfiguracja uprawnień administracyjnych dla funkcji konsoli



Motyw

Dostosowanie logo, kolorów i wyglądu konsoli



Aktualizacje

Zarządzanie aktualizacjami serwera Proget - ręcznymi i automatycznymi

Kontrola dostępu

Zaktualizowano: 3 cze 2026

Opcja pozwala zdefiniować reguły dostępu do usług zarządzania Proget tylko z określonych adresów sieciowych.

Allowed IPs:

123.123.123.123

Add

Disable access control

Submit

1 Dozwolone adresy IP

- Wprowadź adres IP, przez który dozwolone będzie zarządzanie Progetem

2 Usuń

- Usuń wybrany adres IP

3 Dodaj

- Dodaj adres IP

4 Wyłącz kontrolę dostępu

- Usuń wszystkie dodane adresy IP

5 Zapisz

- Zapisz wybrane ustawienia

Dozwolone karty SIM

Zaktualizowano: 3 cze 2026

NOWOŚĆ

Zarządzaj dozwolonymi kartami SIM, które mogą być używane na urządzeniach

Updated

Example Example2026-05-11 12:30:19

ListOperations

1Lista

- Wyświetla listę wszystkich dozwolonych kart SIM (ICCID) dodanych do systemu, z możliwością wyszukiwania po fragmencie numeru ICCID oraz eksportu listy do pliku CSV

2Operacje

- Wyświetla historię operacji masowych wykonanych na liście dozwolonych kart SIM (dodanie, usunięcie, usunięcie wszystkich), wraz z ich statusem, datą utworzenia i zakończenia, liczbą przetworzonych rekordów oraz szczegółami operacji

Lista

Zaktualizowano: 3 cze 2026

Widok Lista wyświetla wszystkie dozwolone karty SIM (numery ICCID) dodane do systemu. Umożliwia wyszukiwanie konkretnego numeru ICCID po fragmencie numeru, zarządzanie listą poprzez operacje masowe, eksport listy do pliku CSV oraz odświeżanie danych.

ListOperations

ICCID: Start typing...

Reset filters

BASICPQL

Manage Allowed SIM Cards

ICCID

123000123000123000

1 Filtr

- Użyj filtra, aby przefiltrować listę dozwolonych kart SIM poprzez wprowadzenie fragmentu numeru ICCID

2 Zarządzaj dozwolonymi kartami SIM

- Ta akcja pozwala otworzyć kreator zarządzania listą dozwolonych kart SIM - dodać nowe numery ICCID, usunąć wybrane lub usunąć wszystkie wpisy z listy

3 Eksportuj

- Ta akcja pozwala wyeksportować aktualną listę dozwolonych kart SIM (numery ICCID) do pliku CSV

4 Odśwież

- Ta akcja pozwala odświeżyć listę dozwolonych kart SIM, aby wyświetlić najnowsze dane

- Wyświetla wszystkie numery ICCID dodane do listy dozwolonych kart SIM

Zarządzaj dozwolonymi kartami SIM

Zaktualizowano: 3 cze 2026

Kreator Zarządzaj dozwolonymi kartami SIM umożliwia wykonywanie operacji masowych na liście dozwolonych kart SIM (numerów ICCID). Możesz dodać nowe wpisy, usunąć wybrane lub usunąć wszystkie wpisy z listy. Nowe numery ICCID można dodawać z pliku CSV lub wprowadzać ręcznie.

Operation type:

☒ Add

☐ Delete

☐ Delete all

☐ From file

☐ Manual input

1 Dodaj

- Ta akcja pozwala dodać nowe numery ICCID do listy dozwolonych kart SIM poprzez import z pliku CSV lub ręczne wprowadzenie

2 Usun

- Ta akcja pozwala usunąć wybrane numery ICCID z listy dozwolonych kart SIM poprzez import z pliku CSV lub ręczne wprowadzenie

3 Usun wszystko

- Ta akcja pozwala usunąć wszystkie numery ICCID z listy dozwolonych kart SIM jednocześnie

4 Z pliku

4.1 Wybierz plik

- Ta akcja pozwala wybrać plik CSV zawierający listę numerów ICCID do dodania lub usunięcia
- Przykładowy plik CSV można pobrać z poziomu kreatora

5 Ręczne wprowadzanie

5.1 Wpisz numer SIM ICCID

- Wprowadź numer ICCID karty SIM, która ma zostać dodana lub usunięta z listy dozwolonych kart SIM

5.2 Dodaj

- Ta akcja pozwala dodać kolejne pole do ręcznego wprowadzania numeru ICCID

Operacje

Zaktualizowano: 3 cze 2026

Widok Operacje wyświetla historię operacji masowych wykonanych na liście dozwolonych kart SIM (dodanie, usunięcie, usunięcie wszystkich). Dla każdej operacji prezentuje typ, datę utworzenia i zakończenia, liczbę przetworzonych rekordów, status oraz szczegóły operacji. Listę można filtrować po statusie oraz odświeżać w celu wyświetlenia najnowszych danych.

ListOperations

Status: Select

Reset filters

BASICPQL

TYPE	CREATION DATE	COMPLETION DATE	PROCESSED	STATUS	DETAILS
Adding	2026-05-11 12:30:18	2026-05-11 12:30:19	1/1	Succeeded	-
Deleting	2026-05-11 04:37:40	2026-05-11 04:37:41	1/1	Succeeded	-
Deleting all	2026-05-11 04:36:56	2026-05-11 04:36:57	3/3	Succeeded	-
Adding	2026-05-11 04:36:35	2026-05-11 04:36:36	0/3	Failed	Show errors
Adding	2026-05-11 04:36:15	2026-05-11 04:36:16	3/3	Succeeded	-

1Filtr

- Użyj filtru, aby filtrować listę operacji po statusie

2Odśwież

- Ta akcja pozwala odświeżyć listę operacji, aby wyświetlić najnowsze dane

3Lista operacji z ich parametrami

- Wyświetla listę operacji masowych wykonanych na liście dozwolonych kart SIM, zawierającą typ operacji, datę utworzenia i zakończenia, liczbę przetworzonych rekordów, status oraz szczegóły operacji

Audyt i logowanie

Zaktualizowano: 12 lut 2025

Proget posiada możliwość rejestrowania dzienników audytu, których możesz użyć do zbadania wszelkich działań administracyjnych i interakcji między serwerem a urządzeniami.

Lista

ListConfiguration

Date: Select date

Reset filters

Selected: 0 | Deselect all

Download

Delete all

☐	FILENAME	DATE	SIZE
☐	audit-2024-10-22.log	2024-10-22	809.46 KIB (828.88 KB)
☐	request-2024-10-22.log	2024-10-22	11.56 KIB (11.84 KB)

Results: 2 | Page limit: 50

<<

<

1

>

>>

1Lista

- Lista utworzonych dzienników zdarzeń

2Pobierz

- Pobierz wybrane dzienniki zdarzeń

3Usuń wszystkie

- Usuń wszystkie dzienniki zdarzeń

Konfiguracja

1 Konfiguracja

- Konfiguracja dzienników zdarzeń

2 Zapisz dzienniki zdarzeń

- Jeśli zaznaczone, dzienniki zdarzeń będą zapisywane i widoczne w zakładce 'Lista'

3 Usuń dzienniki zdarzeń

- Wybierz czas, po którym zapisane dzienniki zdarzeń zostaną usunięte
- Wymagane

Menedżer certyfikatów

Zaktualizowano: 3 gru 2024

Menedżer certyfikatów pozwala na zarządzanie certyfikatami urządzeń i użytkowników, które będą wykorzystywane w profilach i konfiguracjach aplikacji.

CAS

User certificates

External certificates

Name: Start typing...

Common name: Start typing...

Issuer: Start typing...

Created by: Start typing...

Reset filters

Selected: 0

Deselect all

Add

	NAME	COMMON NAME	ISSUER	CREATED BY
>	☐ Example 1	A	Self-signed	John Doe
>	☐ Example 2	AK	Example 1	John Doe

Results: 2

Page limit: 50

1

- 1

CAs
- 2

Certyfikaty użytkownika
- 3

Certyfikaty zewnętrzne

CAs

Zaktualizowano: 14 mar 2025

CA to wewnętrzny urząd certyfikacji, który samodzielnie wystawia i podpisuje certyfikat główny i pośredniczący. Umożliwia generowanie i podpisywanie certyfikatów dla serwerów, użytkowników w ramach zamkniętych systemów organizacji, aby zapewnić zaufanie połączenie. Dzięki obsłudze podpisywania certyfikatów wewnętrznych, CA pozwala na zarządzanie infrastrukturą kluczy publicznych (PKI), wydawanie certyfikatów TLS/SSL, uwierzytelnianie użytkowników oraz zabezpieczanie komunikacji w sieciach prywatnych.

CAs

User certificates

External certificates

Name: Start typing...

Common name: Start typing...

Issuer: Start typing...

Created by: Start typing...

Reset filters

Selected: 1

Deselect all



Add

☒	NAME	COMMON NAME	ISSUER	CREATED BY
☒	Example CA	Example CN	Self-signed	Ironman Ironman

Certificate

CN=Example CN

- CN: Example CN

```
{
  "hash": "a46973c4",
  "name": "/CN=Example CN",
  "validTo": "341119171722Z",
  "version": 2,
  "purposes": {
    "1": [
      true,
      true,
      "sslclient"
    ],
    "2": [
      true,
      true,
      "sslserver"
    ]
  }
}
```

Results: 1

Page limit: 50



1 Eksportuj

- Eksport wybranych certyfikatów CA

2 Generuj certyfikat serwera

2.1 Nazwa

- Nazwa wybranego certyfikatu CA

2.2 Długość klucza

- Wybierz długość klucza
- Jedna z opcji:
 - 1024
 - 2048
 - 3072
 - 4096

2.3 Podpis szyfrujący

- Wybierz typ podpisu szyfrowania
- Jedna z opcji:
 - SHA-1
 - SHA-256
 - SHA-384
 - SHA-512

2.4 Common Name

- Wpisz wspólną nazwę certyfikatu CA
- Maksymalna długość tekstu to 64
- Wymagane

2.5 Ważność (w dniach)

- Minimalna wartość to 30
- Maksymalna wartość to 730
- Wymagane

2.6 Hasło

- Wpisz hasło, które będzie używane do otwarcia pliku

2.7 Typ

- Wybierz typ niestandardowych atrybutów, które są danymi osadzonymi tylko w CSR
- Jedna z opcji:
 - Distinguished_Name
 - NT_principal_Name
 - RFC822_Name
 - DNS_Name

2.8 Wartość

- Wpisz wartość typu
- Dostępne zmienne globalne
- Wymagane

2.9 Usuń

- Usuń wybrany niestandardowy atrybut

2.10 Wyczyść

- Usuń wszystkie niestandardowe atrybuty

2.11 Dodaj

- Dodaj niestandardowy atrybut

3 Informacje o certyfikacie CA

- Główne informacje zawarte w certyfikacie CA

4 Tworzenie CA

4.1 Nazwa

- Wpisz nazwę certyfikatu CA
- Maksymalna długość tekstu to 64
- Wymagane

4.2 Common name

- Wpisz wspólną nazwę certyfikatu CA
- Maksymalna długość tekstu to 64
- Wymagane

4.3 Kod kraju

- Wpisz kod kraju
- Maksymalna długość tekstu to 2

4.4 Województwo

- Wpisz nazwę województwa
- Maksymalna długość tekstu to 128

4.5 Miasto

- Wpisz nazwę miasta
- Maksymalna długość tekstu to 128

4.6 Organizacja

- Wpisz nazwę organizacji

- Maksymalna długość tekstu to 64

4.7 Jednostka organizacyjna

- Wpisz nazwę jednostki organizacyjnej
- Maksymalna długość tekstu to 64

4.8 Długość klucza

- Wybierz jedną z dostępnych długości kluczy
- Wymagane

4.9 Podpis szyfrujący

- Wybierz podpis szyfrujący
- Jedna z opcji:
 - SHA-1
 - SHA-256
 - SHA-384
 - SHA-512
- Wymagane

4.10 Ważność certyfikatu (w dniach)

- Wpisz liczbę dni ważności certyfikatu
- Maksymalna wartość to 3650
- Wymagane

4.11 Certyfikat podpisywania

- Wybierz jeden z dostępnych certyfikatów podpisujących

Certyfikaty użytkownika

Zaktualizowano: 3 gru 2024

Certyfikaty użytkownika określają, do których zasobów dany użytkownik może mieć dostęp.

CAs

User certificates

External certificates

User: Start typing...

Profile: Start typing...

Issuer: Start typing...

Revoked: Select

Reset filters

Selected: 1

Deselect all

☒	USER	PROFILE	ISSUER	VALIDITY	REVOKED	
☒	John Doe	Example cert	Example 1	2025-09-06 13:40:04	-	...

Certificate

CN=jdoe@proget.pl

CN: jdoe@proget.pl

```
{
  "hash": "ed074d66",
  "name": "/CN=jdoe@proget.pl",
  "validTo": "250906114004Z",
  "version": 2,
  "purposes": {
    "1": [
      true,
      false,
      "sslclient"
    ],
    "2": [
      false,
      false,
      "sslsrvr"
    ]
  }
}
```

Results: 1 | Page limit: 50

1

1

Odnów

- Odnawia wybrany certyfikat

2

Unieważnij

- Unieważnienie certyfikatu spowoduje zaprzestanie działania funkcjonalności korzystających z tego certyfikatu.
- Wybrana akcja jest nieodwracalna.

3

Informacje o certyfikacie użytkownika

- Główne informacje zawarte w certyfikacie użytkownika

Zewnętrzne certyfikaty

Zaktualizowano: 3 gru 2024

Typ zewnętrznego certyfikatu jest tutaj zawsze ustawiony jako S/MIME. S/MIME to skrót od Secure/Multipurpose Internet Mail Extensions. Ten typ cyfrowego certyfikatu umożliwia użytkownikom zabezpieczenie integralności i prywatności ich wiadomości e-mail.

CASUser certificatesExternal certificates

User: Start typing...Edited by: Start typing...

Reset filters

Selected: 1Deselect all

Add

☒	USER	TYPE	EDITED BY	VALIDITY	
☒	John Doe	S/MIME	Ironman Ironman	2025-03-07 08:40:27 2025-03-07 08:40:27	...

Signing certificate

CN=test2@bes.pl

CN: test2@bes.pl

```
{
  "hash": "8cd37a72",
  "name": "/CN=test2@bes.pl",
  "validTo": "250307074027Z",
  "version": 2,
  "purposes": {
    "1": [
      false,
      false,
      "sslclient"
    ],
    "2": [
      false,
      false,
      "sslsrvr"
    ]
  }
}
```

Encryption certificate

CN=test2@bes.pl

CN: test2@bes.pl

```
{
  "hash": "8cd37a72",
  "name": "/CN=test2@bes.pl",
  "validTo": "250307074027Z",
  "version": 2,
  "purposes": {
    "1": [
      false,
      false,
      "sslclient"
    ],
    "2": [
      false,
      false,
      "sslsrvr"
    ]
  }
}
```

Results: 1 | Page limit: 50

1

1

Edytuj

- Edytuj wybrany certyfikat

2 Usuń

- Usuń wybrane certyfikaty

3 Informacje o zewnętrznym certyfikacie

- Główne informacje zawarte w zewnętrznym certyfikacie

4 Tworzenie zewnętrznych certyfikatów

4.1 Typ

- Niezmienialny typ zewnętrznego certyfikatu - zawsze ustawiony jako S/MIME

4.2 Użytkownik

- Wybierz jednego z dostępnych użytkowników
- Aby znaleźć użytkownika, wpisz przynajmniej 3 pierwsze litery nazwy użytkownika

4.3 Wybierz plik certyfikatu podpisującego

- Wybierz plik
- Dozwolony typ pliku: .pfx

4.4 Usuń certyfikat podpisujący

- Usuwa wybrany certyfikat podpisujący

4.5 Hasło certyfikatu podpisującego

- Wpisz hasło certyfikatu podpisującego

4.6 Wybierz plik certyfikatu szyfrującego

- Wybierz plik
- Dozwolony typ pliku: .pfx

4.7 Usuń certyfikat szyfrujący

- Usuwa wybrany certyfikat szyfrujący

4.8 **Hasło certyfikatu szyfrującego**

- Wpisz hasło certyfikatu szyfrującego

Connector

Zaktualizowano: 3 gru 2024

Proget Connector to moduł pozwalający na zestawienie połączenia LDAP z sieci lokalnej do serwera znajdującego się w Chmurze Proget.

* Name:	* Address:	* Port:
Example	example.url	123

1 Nazwa

- Wprowadź nazwę Connectora
- Maksymalna długość tekstu to 255
- Wymagane

2 Adres

- Wprowadź adres serwera
- Maksymalna długość tekstu to 255
- Wymagane

3 Port

- Wprowadź numer portu, który jest częścią informacji adresowych używanych do identyfikacji odbiorców i nadawców wiadomości sieciowych
- Minimalna wartość to 0
- Maksymalna wartość to 65535
- Wymagane

Gateway

Zaktualizowano: 3 gru 2024

Bezpieczna brama dostępowa dla poczty email, która szyfruje i zabezpiecza ruch pomiędzy urządzeniem mobilnym a wewnętrznymi systemami pocztowymi.

* Gateway name: Example	* Access server address: Example Access server address * Access server port: ⓘ 443 * Email server address: Example Email Server Address * Email server port: 443	* Authentication: Local CA SCEP: Select Root certificate: ⓘ Select CA: Select
---	--	---

1

Nazwa

1.1

Nazwa

- Nazwa bramy
- Maksymalna długość 255
- Wymagane

2

Poświadczenia

2.1 Adres serwera dostępowego

- Wprowadź adres serwera dostępu
- Maksymalna długość tekstu to 255
- Wymagane

2.2 Port serwera dostępowego

- Wprowadź port serwera dostępu
- Maksymalna wartość to 65535
- Wymagane

2.3 Adres serwera pocztowego

- Wprowadź adres serwera e-mail
- Maksymalna długość tekstu to 255
- Wymagane

2.4 Port serwera pocztowego

- Wprowadź port serwera e-mail
- Maksymalna wartość to 65535
- Wymagane

3 Poświadczenia

3.1 Uwierzytelnienie

- Wybierz metodę autentykacji
- Jedna z:
 - Lokalne CA
 - Enterprise CA
 - Menedżer certyfikatów
- Wymagane

3.2 SCEP

- Wybierz jeden z dostępnych profili SECEP
- Dostępne, jeśli wybrano metodę uwierzytelnienia Enterprise CA
- Wymagane, jeśli wybrano metodę uwierzytelnienia Enterprise CA

3.3 Certyfikat główny

- Wybierz jeden z dostępnych profili Certyfikatu
- Dostępne, jeśli wybrano metodę uwierzytelnienia Enterprise CA
- Wymagane, jeśli wybrano metodę uwierzytelnienia Enterprise CA

3.4 CA

- Wybierz jeden z dostępnych certyfikatów CA
- Dostępne, jeśli wybrano metodę uwierzytelnienia Menedżer certyfikatów
- Wymagane, jeśli wybrano metodę uwierzytelnienia Menedżer certyfikatów

Ogólne

Zaktualizowano: 3 cze 2026

Informacje o serwerze oraz jego konfiguracja.

Organization

Server

Application

TURN

* Organization name:

Example Company

Email address:

mail@example.com

Phone:

+48 123 123 123

* Country: ⓘ

United Kingdom

▼

* City:

Example city

* Street:

Example

* Postal Code:

12-345

* House number:

123

1.1 Nazwa organizacji

- Wprowadź nazwę organizacji
- Maksymalna długość tekstu to 128
- Wymagane

1.2 Adres email

- Jeśli wprowadzony, będzie widoczny w aplikacji Proget
- Maksymalna długość tekstu to 128

1.3 Telefon

- Jeśli wprowadzony, będzie widoczny w aplikacji Proget
- Maksymalna długość tekstu to 64

1.4 Kraj

- Wybierz jeden z krajów
- Wybranie kraju dostosuje wyświetlane w konsoli mapy
- Wymagane

1.5 Miasto

- Wprowadź nazwę miasta
- Maksymalna długość tekstu to 64
- Wymagane

1.6 Kod pocztowy

- Wprowadź kod pocztowy
- Maksymalna długość tekstu to 64
- Wymagane

1.7 Ulica

- Wprowadź nazwę ulicy
- Maksymalna długość tekstu to 64
- Wymagane

1.8 Nr domu

- Wprowadź numer domu
- Maksymalna długość tekstu to 64
- Wymagane

2 Serwer

2.1 Strefa czasowa

- Wybierz jedną ze stref czasowych
- Wymagane

2.2 Język domyślny

- Wybierz domyślny język - domyślny język określa, w jakim języku będą domyślne zasady i informacje pobierane ze sklepów aplikacji
- Jeden z:
 - Polski
 - Angielski
 - Niemiecki
 - Rosyjski
 - Rumuński

2.3 Włącz Cloudflare captcha podczas logowania

- Ta opcja pozwala włączyć mechanizm Cloudflare captcha podczas logowania do systemu

2.4 Akcje dla nieaktywnych urządzeń

- Wybierz działanie, które zostanie wysłane do nieaktywnego urządzenia próbującego połączyć się z serwerem. Dostępne dla urządzeń z systemem Windows i Android. Urządzenia iOS, macOS zawsze otrzymają akcję wyczyszczenia danych służbowych.
- Jeden z:
 - Nie podejmuj akcji
 - Wyczyść dane służbowe
 - Wyczyść dane urządzenia
- Wymagane

2.5**Przywracanie danych służbowych w przypadku błędu synchronizacji aplikacji Proget**

- W przypadku błędu synchronizacji aplikacji Proget, użytkownik może ręcznie przywrócić dane służbowe. Dzięki tej funkcjonalności nie będzie wymagane przywrócenie urządzenia do ustawień fabrycznych, aby ponownie zarejestrować się w konsoli Proget.
- Jeden z:
 - Zawsze pozwalaj
 - Pozwalaj po podaniu kodu zabezpieczeń
 - Nie pozwalaj **Przestarzała**
- Wymagane

2.6**Certyfikat SSL konsoli**

- Wybierz certyfikat SSL dla konsoli z zasobów Twojego urządzenia. Zostaniesz poproszony o podanie hasła certyfikatu oraz hasła użytkownika.

3**Aplikacja**

3.1 Adres do aplikacji Android

- Wprowadź adres do aplikacji Android
- Maksymalna długość tekstu to 255

3.2 Lokalizacja sklepu z aplikacjami

- Wybierz jeden z krajów - lokalizacja sklepu z aplikacjami określa kraj/region wyszukiwania aplikacji w sklepie. Funkcja może wpłynąć na brak dostępu do aplikacji niedostępnych w danym kraju/regionie.

3.3 Numer ratunkowy

- Wprowadzony numer będzie widoczny jako numer alarmowy na ekranie blokady urządzenia
- Maksymalna długość numerów to 16
- Wymagane

4 Turn

4.1 URL

- Wprowadź URL TURN
- Poprawny URL jest wymagany, jeśli administrator konsoli Proget chce korzystać z Proget Remote
- Maksymalna długość tekstu to 128
- Wymagane

4.2 Nazwa użytkownika

- Wprowadź nazwę użytkownika TURN
- Poprawna nazwa użytkownika TURN jest wymagana, jeśli administrator konsoli Proget chce korzystać z Proget Remote
- Wymagane

4.3 Zmień hasło

- Wprowadź nowe hasło
- Maksymalna długość tekstu to 256
- Dostępne, jeśli zaznaczone pole wyboru
- Wymagane, jeśli zaznaczone pole wyboru

4.4 Przywróć ustawienia domyślne

- Przywraca wartości domyślne

5 Wybierz certyfikat

5.1 Wybierz plik

- Wybierz plik, który chcesz przesłać
- Dozwolony typ pliku: .pfx

5.2 Hasło certyfikatu

- Wprowadź hasło certyfikatu
- Wymagane

5.3 Hasło użytkownika

- Wprowadź hasło użytkownika
- Wymagane

LDAP

Zaktualizowano: 24 cze 2025

Zarządzaj połączeniami LDAP do synchronizacji usług katalogowych.

* Name:

Example

SERVER AND ENCRYPTION

☒ Active Directory

* Domain:

domain.example

* Host name:

Example hostname

* Port:

443

Base dn:

Search Filter:

(&(objectclass=person)(objectclass=user))

* Search Scope:

All Levels

* Encryption:

None

Connector:

No Connectors configured

☒ Accept untrusted connections

CA certificate file (LDAP SSL/TLS):

Select file Not selected

USER

User:

Example user

Password:

User attributes:

Add

Sync users

Users:

☒ Sync everyone

☐ Sync existing

* Tolerance (in hours, 1-24):

1

☒ Send notification to users about adding an account in the Proget system

☒ Send activation to users ⓘ

* Activation selection:

Android

Assign label:

user

☒ Send notifications about changes

☒ Actions on deleting a user

* Actions:

Unassign labels

1 Nazwa

- Podaj nazwę konfiguracji LDAP
- Maksymalna długość tekstu to 64
- Wymagane

2 Serwer i szyfrowanie

2.1 Active Directory

- Jeśli zaznaczone, LDAP będzie skonfigurowany jako Active Directory

2.2 Domena

- Wprowadź adres domeny
- Maksymalna długość tekstu to 64
- Wymagane, jeśli Active Directory jest zaznaczone

2.3 Nazwa hosta

- Wprowadź nazwę hosta
- Maksymalna długość tekstu to 255
- Wymagane

2.4 Port

- Wprowadź port serwera
- Maksymalna wartość to 65535
- Wymagane

2.5 Base dn

- Wprowadź podstawowy dn
- Maksymalna długość tekstu to 255

2.6 Filtr wyszukiwania

- Wprowadź filtr wyszukiwania
- Maksymalna długość tekstu to 255

2.7 Zakres wyszukiwania

- Wybierz zakres wyszukiwania
- Jedno z:
 - Wszystkie poziomy
 - Jeden poziom
- Wymagane

2.8 Szyfrowanie

- Wybierz szyfrowanie
- Jedno z:
 - Brak
 - SSL
 - TLS
- Wymagane

2.9 Connector

- Wybierz jeden z podanych łączników

2.10 Akceptuj niezaufane połączenia

- Jeśli zaznaczone, niezaufane połączenia będą przepuszczane

2.11 Wybierz plik

- Wgrywa plik certyfikatu CA (LDAP SSL/TLS)

3 Poświadczenia

3.1 Użytkownik

- Wprowadź poświadczenia użytkownika

3.2 Hasło

- Wprowadź hasło

3.3 Atrybuty użytkownika

- Wprowadź atrybuty użytkownika
- Dostępne, jeśli zaznaczone Active Directory

3.4 Usuń

- Usuń wybrane atrybuty użytkownika

3.5 Dodaj

- Dodaj więcej atrybutów użytkownika

4 Synchronizacja

4.1 Synchronizuj użytkowników

- Jeśli zaznaczone, użytkownicy będą synchronizowani

4.2 Synchronizuj wszystkich

- Jeśli zaznaczone, wszyscy użytkownicy będą synchronizowani

4.3 Synchronizuj istniejących

- Jeśli zaznaczone, istniejący użytkownicy będą synchronizowani

4.4 Tolerancja

- Wybierz tolerancję synchronizacji (w godzinach)
- Minimalna wartość to 1
- Maksymalna wartość to 24
- Wymagane

4.5 Przypisz etykietę

- Wybierz jedną z dostępnych etykiet
- Dostępne, jeśli zaznaczone Synchronizuj użytkowników

4.6 Wyślij powiadomienia

- Jeśli zaznaczone, system wyśle powiadomienie do użytkowników o dodaniu konta w systemie Proget
- Aby ta funkcja działała prawidłowo, należy skonfigurować SMTP w zakładce Ustawienia
- Dostępne, jeśli zaznaczone Synchronizuj użytkowników

4.7 Wyślij powiadomienia o zmianach

- Jeśli zaznaczone, powiadomienia o zmianach zostaną wysłane

- Aby ta funkcja działała prawidłowo, należy skonfigurować SMTP w zakładce Ustawienia.
- Dostępne, jeśli zaznaczone Synchronizuj użytkowników

4.8 Wyślij aktywację użytkownikom

- Jeśli zaznaczone, aktywacje zostaną wysłane do wybranych poniżej typów użytkowników aktywacji
- Aby ta funkcja działała prawidłowo, należy skonfigurować SMTP w zakładce Ustawienia. Jeśli chcesz wysłać aktywację Android Enterprise, iOS lub macOS wymagane jest dodanie odpowiedniej integracji w zakładce Integracje.
- Dostępne, jeśli zaznaczone Synchronizuj użytkowników

4.9 Akcje przy usunięciu użytkownika

- Jeśli zaznaczone, zostaną wykonane działania przy usuwaniu użytkownika
- Dostępne, jeśli zaznaczone Synchronizuj użytkowników

4.10 Wybór aktywacji

- Wybierz aktywację
- Jedno z:
 - Android Enterprise Device Owner
 - Android Enterprise Profile Owner
 - Android
 - iOS
 - macOS
 - Windows
- Dostępne, jeśli zaznaczone Synchronizuj użytkowników i Wyślij aktywację użytkownikom
- Wymagane, jeśli zaznaczone Wyślij aktywację użytkownikom

4.11 Akcje

- Jeśli zaznaczone, zostaną wykonane działania przy usuwaniu użytkownika

- Usuń użytkownika
 - Odepnij urządzenia
 - Wyczyść dane urządzenia
 - Wyczyść dane służbowe
 - Odepnij etykiety
 - Zablokuj użytkownika
- Dostępne, jeśli zaznaczone Synchronizuj użytkowników i Działania przy usuwaniu użytkownika
 - Wymagane, jeśli zaznaczone Działania przy usuwaniu użytkownika

Microsoft Entra ID

Zaktualizowano: 3 gru 2024

Zarządzanie połączeniem i synchronizacją z Microsoft Entra ID.

Users configurations

Settings

- 1

Konfiguracje użytkowników
- 2

Ustawienia

Konfiguracje użytkowników

Zaktualizowano: 3 gru 2024

Name:

Example Entra Id configuration

* Microsoft Entra ID Application: ⓘ

Entra

▼

* Filter:

Group users

▼

* Group ID: ⓘ

Example groups filter

User attributes: ⓘ

\$filter=

SYNCHRONIZATION:

☒ Sync users

☒ Send notification to users about adding an account in the Proget system ⓘ

Assign label:

user

X ▼

Send activation to users: ⓘ

Android Enterprise Profile Owner

X ▼

Actions on deleting a user:

Remove label

X ▼

☐ Send notifications about changes ⓘ

USERS MAPPING:

Field in Proget Console

Email address

Username

First name

Surname

* Field in Microsoft Entra ID

mail

mailNickname

givenName

surname

Add

☒ Map local users

1

- Nazwa Microsoft Entra ID
- Maksymalna długość tekstu to 255
- Wymagane

2

2.1 Microsoft Entra ID Application

- Wybierz jedną z dostępnych aplikacji
- Dostępne są tylko aplikacje Microsoft Entra ID z przypisanymi uprawnieniami: Group.Read.All, User.Read.All
- Wymagane

2.2 Filtr

- Filtruj po:
 - Wszyscy użytkownicy
 - Użytkownicy grupy
 - Atrybuty użytkownika

2.3 Group ID

- Filtr pozwala ograniczyć dodawanie i synchronizację użytkowników Microsoft Entra ID do tych, którzy są członkami określonej grupy. Chcąc filtrować użytkowników względem przynależności do określonej grupy Microsoft Entra ID, wprowadź Identyfikator Grupy. Przykład: e15b8ad0-d4c1-11ed-b7a7-e8d8d1e95e11. Identyfikator Grupy znajdziesz logując się do <https://portal.azure.com>, a następnie przechodząc do Microsoft Entra ID > Grupy > Wybierz grupę > Przegląd > Identyfikator obiektu. Kliknij w 'i' aby przejść do Portalu Microsoft Entra ID.

2.4 User attributes

- Filtr pozwala ograniczyć dodawanie i synchronizację użytkowników Microsoft Entra ID do tych, którzy posiadają określone atrybuty. Utwórz filtr korzystając z obsługiwanych atrybutów i operatorów. Przykład: department eq 'Dział marketingu'. Kliknij w 'i' aby przejść do dokumentacji Microsoft.

2.5 Synchronizuj użytkowników

- Jeśli zaznaczone, użytkownicy są synchronizowani

2.6 Wyślij powiadomienie użytkownikom o dodaniu konta w systemie Proget

- Jeśli zaznaczone, powiadomienia są wysyłane do użytkowników
- Aby ta funkcja działała prawidłowo, należy skonfigurować SMTP w zakładce Ustawienia

2.7 Przypisz etykietę

- Wybierz jedną z dostępnych etykiet

2.8 Wyślij aktywację użytkownikom

- Wybierz typ aktywacji
- Jedno z:
 - Android
 - Android Enterprise Device Owner
 - Android Enterprise Profile Owner
 - iOS
 - macOS
 - Windows
- Aby ta funkcja działała poprawnie, należy skonfigurować SMTP w zakładce Ustawienia. Jeśli chcesz wysłać aktywację Android Enterprise, iOS lub macOS wymagane jest dodanie odpowiedniej integracji w zakładce Integracje.

2.9 Akcje przy usunięciu użytkownika

- Wybierz akcję, która zostanie wykonana po usunięciu użytkownika
- Jedno z:
 - Usuń etykietę i wyczyść dane służbowe z urządzeń
 - Usuń etykietę i wyczyść dane urządzenia
 - Usuń etykietę

2.10 Wyślij powiadomienia o zmianach

- Jeśli zaznaczone, powiadomienia o zmianach są wysyłane
- Aby ta funkcja działała prawidłowo, należy skonfigurować SMTP w zakładce Ustawienia

3 Mapowanie użytkowników

3.1 Pole z konsoli Proget

- Pole z konsoli Proget używane do mapowania użytkowników z Microsoft Entra ID

3.2 Pole z Microsoft Entra ID

- Wybierz jedno z pól dostępnych w Microsoft Entra ID używanych do mapowania użytkowników do konsoli Proget
- Wymagane

3.3 Usuń

- Usuwa odpowiadającą linię z polami dla mapowania użytkowników
- Odblokowane tylko dla pól dodanych przez użytkownika

3.4 Dodaj

- Dodaje nową linię z polami dla mapowania użytkowników

3.5 Mapuj lokalnych użytkowników

- Jeśli zaznaczone, lokalni użytkownicy są mapowani

Ustawienia

Zaktualizowano: 3 cze 2026

Users configurations

Settings

☒ Enable sign-in with Microsoft Entra ID

Devices synchronization application: ⓘ

Select

During verification, you will be redirected to Microsoft Entra ID. To authorize your access ensure account you are using has Global Admin Rights. Otherwise, you will be able to send only a request to the Microsoft Entra ID administrator.

 Verify Proget application

1 Włącz logowanie za pomocą usługi Azure AD

- Jeśli zaznaczone, możesz zalogować się do konsoli Proget za pomocą usługi Azure AD

2 Aplikacja do synchronizacji urządzeń

- Wybierz jedną z dostępnych aplikacji
- Dostępne są tylko aplikacje Azure AD z przypisanymi uprawnieniami: Device.ReadWrite.All

3 Zweryfikuj aplikację Proget

- Zweryfikuj wybraną aplikację Proget na portalu Microsoft Azure. Upewnij się, że masz uprawnienia Global Admin Rights.

Role

Zaktualizowano: 3 cze 2026

Role pozwalają na konfigurację uprawnień administracyjnych do przeglądania, oraz zarządzania zawartością dla poszczególnych funkcji konsoli

Selected: 0 | Deselect all



Add

☐	NAME	LABELS
☐	Admin	admin
☐	User	user

Results: 2 | Page limit: 50

<<

<

1

>

>>

1 Kopiuuj

- Ta akcja pozwala na skopiowanie wybranej roli z listy

2 Edytuj

- Ta akcja pozwala na edycję wybranej roli z listy

3 Usun

- Ta akcja pozwala na usunięcie wybranych ról z listy

4 Dodaj

- Klikając w ten przycisk, zostaniesz przeniesiony do etapów tworzenia nowej roli

5 Lista ról

- Lista ról, które zostały utworzone wraz z przypisanymi do nich etykietami

Dodaj rolę

Zaktualizowano: 3 cze 2026

Add role

* Name:

Enable two-factor authentication: ☒

Allow multiple sessions: ☒

Inactivity time:

Labels:

Back

Submit

1 Nazwa

- Wprowadź nazwę roli
- Maksymalna długość tekstu to 32
- Wymagane

2 Włącz uwierzytelnianie dwuetapowe

- Zaznacz pole wyboru, jeśli chcesz włączyć uwierzytelnianie dwuetapowe podczas logowania do konsoli

3 Pozwalaj na wiele sesji

- Zaznacz pole wyboru, jeśli chcesz pozwolić na wiele sesji jednocześnie

4 Czas nieaktywności

- Ustaw czas nieaktywności, po którym użytkownik zostanie wylogowany z konsoli
 - 15 minut
 - 30 minut
 - 45 minut
 - 1 godzina
 - 1 godzina 15 minut

- 1 godzina 30 minut
- 1 godzina 45 minut
- 2 godziny

5 Etykiety

- Wybierz etykietę, aby powiązać ją z rolą

6 Wstecz

- Ta akcja pozwala na powrót do poprzedniego widoku, bez zapisywania wprowadzonych wartości

7 Zapisz / Ustawienia roli

7.1 Nazwa

- Wprowadź nazwę roli
- Maksymalna długość tekstu to 32
- Wymagane

7.2 Konfiguracja roli

- Tutaj możesz przypisać etykiety do roli, dla których została utworzona konfiguracja, oraz zarządzać jej podstawowymi parametrami

7.3 Zarządzanie rolami

- Tutaj możesz zarządzać rolami, określając poziom dostępu użytkownika do funkcji konsoli Proget. Każde zaznaczone pole wyboru przyznaje większe uprawnienia

SMTP

Zaktualizowano: 9 paź 2025

Konfiguracja usługi SMTP służącej do wysyłania wiadomości aktywacyjnych oraz powiadomień do użytkownika przy użyciu poczty email.

- ☐ Default configuration
- ☐ Basic authentication
- ☐ Modern authentication (Google)
- ☐ Modern authentication (Microsoft 365)

1 Domyślna konfiguracja

2 Basic authentication

3 Modern authentication (Google)

4 Modern authentication (Microsoft 365)

Domyślna konfiguracja

Zaktualizowano: 9 paź 2025

Domyślna konfiguracja skonfigurowana przez Proget umożliwia wysłanie wiadomości e-mail podczas tworzenia nowego użytkownika w systemie oraz dla resetu hasła użytkownika lokalnego

 Default configuration

 The SMTP default configuration allows the local user's password to be reset and emails to be sent when the user is created.

1 Domyślna konfiguracja

- Jeśli włączona, na serwerze będzie obowiązywać domyślna konfiguracja SMTP, skonfigurowana przez Proget

Basic authentication

Zaktualizowano: 3 gru 2024

Autentykacja SMTP, często skracana do SMTP AUTH, to rozszerzenie protokołu Simple Mail Transfer Protocol (SMTP), umożliwiające klientowi logowanie się przy użyciu dowolnego mechanizmu uwierzytelniania obsługiwanego przez serwer.

Basic authentication

Displayed sender name:

Example

* Sender's email:

user@example.com

* SMTP server:

mail.example.com

* SMTP port:

123

User:

Example

Password:

.....

☐ Allow untrusted connections

Encryption type:

TLS

1

Informacje nadawcy

1.1 Wyświetlana nazwa wysyłającego

- Wprowadź nazwę, która będzie widoczna w wiadomościach email jako nadawca

1.2 Adres email wysyłającego

- Wprowadź email, który będzie widoczny w wiadomościach email jako email nadawcy
- Maksymalna długość tekstu to 64
- Wymagane

1.3 Serwer SMTP

- Wprowadź serwer SMTP
- Maksymalna długość tekstu to 64
- Wymagane

1.4 Port SMTP

- Wprowadź port SMTP
- Wymagany numer
- Wymagane

2 Dane uwierzytelniające użytkownika

2.1 Użytkownik

- Wprowadź email użytkownika, z którego będą wysyłane wiadomości email

2.2 Hasło

- Jeśli zaznaczone, będzie możliwa zmiana hasła

2.3 Zmień hasło

- Wprowadź hasło do emaila, z którego będą wysyłane wiadomości email

3 Ustawienia dodatkowe

3.1 Zezwól na niezaufane połączenia

- Jeśli zaznaczone, połączenia niezaufane będą dozwolone

3.2 Typ szyfrowania

- Wprowadź typ szyfrowania, który zabezpieczy wiadomości email
- Jedno z:
 - Brak
 - SSL
 - TLS

Modern authentication (Google)

Zaktualizowano: 3 gru 2024

SMTP Modern Authentication (Google) to zaawansowana metoda uwierzytelniania klientów SMTP przy użyciu kont Google, zastępująca tradycyjne metody autentykacji loginem i hasłem bardziej bezpiecznymi i elastycznymi mechanizmami, takimi jak OAuth 2.0, co zapewnia lepsze zabezpieczenia oraz integrację z infrastrukturą uwierzytelniania Google.

 Modern authentication (Google)

Displayed sender name:

* Sender's email:
 Sign in with Google

1 Wyświetlana nazwa wysyłającego

- Wprowadź nazwę, która będzie widoczna w wiadomościach email jako nadawca

2 Adres email wysyłającego

- Zaloguj się przy użyciu konta Google, z którego tworzone wiadomości email będą wysyłane z konsoli Proget
- Wymagane

Modern authentication (Microsoft 365)

Zaktualizowano: 3 gru 2024

SMTP Modern Authentication (Microsoft) to zaawansowana metoda uwierzytelniania klientów SMTP przy użyciu poświadczeń Microsoft Entra ID (Microsoft 365), pozwalająca użytkownikom na autentykację za pomocą tokenów Microsoft Entra ID zamiast tradycyjnego loginu i hasła, co zapewnia lepsze zabezpieczenia oraz integrację z zaawansowanymi funkcjami Microsoft Entra ID.

 Modern authentication (Microsoft 365)

Displayed sender name:

* Sender's email:

 Microsoft 365

1 Wyświetlana nazwa wysyłającego

- Wprowadź nazwę, która będzie widoczna w wiadomościach email jako nadawca

2 Adres email wysyłającego

- Zaloguj się przy użyciu konta Microsoft, z którego tworzone wiadomości email będą wysyłane z konsoli Proget
- Wymagane

Motyw

Zaktualizowano: 3 gru 2024

Motywy pozwalają na swobodną modyfikację układu graficznego konsoli Proget. Opcja ta pozwala, między innymi, na wstawienie własnego logo i modyfikację kolorów na całej konsoli. Umożliwia to dostosowanie systemu do potrzeb firmy.

COLOR:

#5c1a51

Set default

LOGO: ⓘ



Select file

Set default

DARK THEME LOGO: ⓘ



Select file

Set default

FAVICON: ⓘ



Select file

Set default

Submit

1 Kolor

1.1 Wybór koloru

- Wybierz kolor systemu Proget

1.2 Ustaw domyślne

- Przywraca domyślne ustawienia

2 Logo

2.1 Podgląd logo

- Pokazuje podgląd wybranego pliku

2.2 Wybierz plik

- Aktualizuje logo z wybranego pliku

2.3 Ustaw domyślne

- Przywraca domyślne logo

3 Dark theme logo

3.1 Podgląd logo dla ciemnego motywu

- Pokazuje podgląd wybranego pliku

3.2 Wybierz plik

- Aktualizuje logo z wybranego pliku

3.3 Ustaw domyślne

- Przywraca domyślne logo dla ciemnego motywu

4 Favicon

4.1 Podgląd favicon

- Pokazuje podgląd wybranego pliku

4.2 Wybierz plik

- Aktualizuje favicon z wybranego pliku

4.3 Ustaw domyślne

- Przywraca domyślny favicon

Aktualizacje

Zaktualizowano: 12 lut 2025

Moduł zarządza aktualizacjami serwera Proget. Aktualizacje można przeprowadzać manualnie lub skonfigurować aktualizacje automatyczne.

Konfiguracja aktualizacji

UPDATE TYPE

☒ Manual

* Version:

Select version

* Update at:

2025-01-01

☐ Automatic

Days:

☐ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

☐ Sunday

Hour:

00:00

1 Ręczne

1.1 Manualne

- Jeśli zaznaczone, ustawienia wprowadzane są ręcznie

1.2 Wersja

- Wybierz, której wersji konsoli Proget będzie używane

1.3 Data i godzina

- Wybierz, kiedy ma nastąpić aktualizacja (data i godzina)

2 Automatyczne

2.1 Automatyczne

- Jeśli zaznaczone, ustawienia wprowadzane są automatycznie

2.2 Dni tygodnia

- Wybierz, w który dzień ma nastąpić aktualizacja, jeśli dostępna jest nowa wersja konsoli Proget

2.3 Godzina

- Wybierz, o której godzinie ma nastąpić aktualizacja, jeśli dostępna jest nowa wersja konsoli Proget

Zaplanowana aktualizacja

1 Aktualizuj teraz

- Aktualizuje konsolę Proget do najnowszej wersji
- Dostępne, jeśli dostępna jest nowa wersja konsoli Proget

2 Zapisz

- Przesyła zmiany poprzez dodanie konfiguracji
- Dostępne, jeśli dodawana jest nowa konfiguracja

3 Usuń

- Usuwa bieżącą konfigurację
- Dostępne, jeśli konfiguracja jest zapisana

Integracje

Zaktualizowano: 16 lip 2026



Android Enterprise

Rozszerzone zabezpieczenia, zarządzanie i obsługa aplikacji Android



Android zero-touch

Bezproblemowe wdrażanie firmowych urządzeń Android metodą zero-touch



Apple Business Manager

Automatyczna aktywacja urządzeń Apple i zdalny tryb nadzorowany



Apple Push Notification Service

Włączenie protokołu MDM do zdalnych poleceń zarządzania



Apps and Books

Hurtowy zakup i dystrybucja aplikacji bez konta iTunes



Microsoft Entra ID Applications

Powiązanie Proget z Entra ID i import użytkowników



Samsung KME

Szybka, automatyczna rejestracja urządzeń po numerze IMEI lub...

Android Enterprise

Zaktualizowano: 3 gru 2024

Integracja z Android Enterprise udostępnia rozszerzone funkcje zabezpieczeń, zarządzania oraz obsługi aplikacji.

Android Enterprise Status: Configured	Organization ID: xxxxxxxxxxxx	Android Enterprise Email: pawel.dawson@gmail.com
--	----------------------------------	---

Remove configuration

DEVICE OWNER  Download QR code Show content	PROFILE OWNER ⓘ Available since Android 10  Download QR code Show content
--	--

☐ Automatically connect to the network ⓘ

SSID:

☐ Hidden network

Security type:

None

Password:

HOW TO ACTIVATE?

1

 Activate the device with a QR code by scanning chosen code.

2

 Launch of a QR code scanner is possible from the device setup start screen ("Welcome!" screen).

3

 Activate the QR code scanner with a few clicks on the welcome screen (any of empty space).

1 Usuń konfigurację

- Usuwa konfigurację Android Enterprise

2 Pobierz kod QR

- Pobiera kod QR w formacie .pdf do aktywacji Device Owner

3 Pokaż zawartość

- Wyświetla informacje zawarte w kodzie QR do aktywacji Device Owner

4 Pobierz kod QR

- Pobiera kod QR w formacie .pdf do aktywacji Profile Owner

5 Pokaż zawartość

- Wyświetla informacje zawarte w kodzie QR do aktywacji Profile Owner

6 Automatyczne połączenie z siecią

- Pozwala na dodanie poświadczeń Wi-Fi do kodu QR, aby automatycznie połączyć się z siecią Wi-Fi podczas rejestracji. Kod QR będzie zawierać niezaszyfrowane hasło do Wi-Fi.

7 SSID

- Wpisz nazwę identyfikującą sieć bezprzewodową.

8 Ukryta sieć

- Wymagane, jeśli sieć, dla której przygotowujemy konfigurację, ukrywa SSID

9 Typ zabezpieczeń

- Jeden z:
 - Brak

- Osobiste WPA/WPA2
- Jeśli wybrano 'Brak', sieć będzie bez zabezpieczeń
- Jeśli wybrano 'Osobiste WPA/WPA2', zarządzanie uwierzytelnianiem użytkownika odbywa się za pomocą klucza WPA pre-shared

10 Klucz wstępny

- Jeśli wybrano 'Osobiste WPA/WPA2', wpisz hasło do sieci bezprzewodowej.

11 Jak aktywować?

- Poniższa instrukcja pomoże ci pobrać aplikację Proget na twoje urządzenie mobilne z Androidem w wybranym trybie.
- Jednym ze sposobów aktywacji urządzenia jest zeskanowanie kodu QR w wybranym typie aktywacji, co spowoduje pobranie i instalację aplikacji Proget (po zeskanowaniu kodu QR nie można zmienić typu aktywacji). Aby uruchomić skaner kodów QR, urządzenie musi być przywrócone do ustawień fabrycznych. Aktywacja skanera kodu QR jest możliwa poprzez kilkukrotne kliknięcie na ekranie powitalnym (dowolne puste miejsce na ekranie).
- Aby zakończyć aktywację urządzenia, zeskanuj mały kod QR dla wcześniej wybranego typu aktywacji lub dodaj urządzenie do automatycznej rejestracji. Mały kod QR można wygenerować klikając na przycisk 'Generuj Aktywację' na karcie użytkownika.

Android zero-touch

Zaktualizowano: 3 gru 2024

Android zero-touch oferuje bezproblemowe wdrażanie dla firmowych urządzeń z systemem Android, dzięki czemu wdrażanie urządzeń na dużą skalę jest szybkie, łatwe i bezpieczne dla organizacji, IT i pracowników. Zero-touch ułatwia konfigurowanie urządzeń online i wysyłanie ich z wymuszonym zarządzaniem przez Proget. Aby aktywować usługę rejestracji urządzeń zero-touch w konsoli Proget, postępuj zgodnie z instrukcją

About zero-touch enrollment

Simplifying zero-touch registration requires a few steps.

- ❶ Sign in to the zero-touch enrollment portal (<https://partnerdash.google.com/zerotouch>) and create a configuration profile.
- ❷ Fill in the required fields of the form.
 - Configuration name: <name of your configuration>
 - EMM DPC: Proget
 - DPC - additional information:

```
{
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
  }
}
```
 - Company name: <shown on the boot screen of the Android device in the help section>
 - Support email address: <shown on the boot screen of the Android device in the help section>
 - Support phone number: <shown on the Android device boot screen in the help section>
- ❸ Set the created configuration as default.
- ❹ Purchase an Android device from an authorized reseller who will add it to your zero-touch console ([Android Enterprise Solutions Directory - Resellers](#)).
- ❺ Turn on your Android device and start setting it up. Zero-touch will force remote device management by Proget. Add the Device auto enrollment in the Proget console to further automate the device registration.

If you need help or want more details, please visit the [Technical Support](#) page for more resources.

Apple Business Manager

Zaktualizowano: 12 lut 2025

Program umożliwia automatyczne aktywowanie urządzeń Apple na serwerze Proget podczas uruchamiania urządzenia lub po przywróceniu ustawień fabrycznych urządzenia. Program umożliwia również zdefiniowanie etapów pierwszego uruchomienia urządzenia oraz zdalne uruchomienie trybu nadzorowanego.

Status: Connected	Expiration date: 2025-01-15
Renew the Proget server communication with the Apple Business Manager account Remove the account association Synchronize	

1 Odnów komunikację serwera Proget z kontem Apple Business Manager

- Ta akcja pozwala na odnowienie komunikacji serwera Proget z Apple Business Manager

2 Usuń powiązanie

- Ta akcja usuwa powiązanie konta

3 Synchronizuj

- Ta akcja synchronizuje serwer Proget i konto Apple Business Manager
-

1 Przejdź do portalu Apple

- Ta akcja przekierowuje do portalu Apple, gdzie można utworzyć konto

2 Pobierz publiczny klucz serwera

- Ta akcja pozwala na pobranie publicznego klucza serwera, który będzie używany w konsoli Apple do wygenerowania tokenu. Ten token będzie wymagany w czwartym kroku.

3 Importuj plik serwera Apple Business Manager (.p7m)

- Ta akcja umożliwia przesłanie na serwer Proget tokenu Apple Business Manager pobranego z konsoli Apple, aby połączyć serwer Proget i serwer Apple

Apple Push Notification Service

Zaktualizowano: 12 lut 2025

Integracja usługi Apple Push Notification umożliwia korzystanie z protokołu MDM, który pozwala na wykonywanie zdalnych poleceń zarządzania.

Apple Push Notification service status: Apple Push Notification service certificate installed	Expiration date: 2025-01-15 10:57:22	Uid: com.apple.mgmt.External.c4753e35-7e47-4db7-86ce-20d916b2926b	Apple ID: No info
Renew certificate Remove integration Edit Apple ID			

1

Odnów certyfikat

- Ta akcja odnawia certyfikat

2

Usuń integrację

- Ta akcja usuwa integrację

3

Edytuj Apple ID

- Ta akcja edytuje Twoje Apple ID
-

1 Generuj Apple Push Notification service certificate signing request

- Ta akcja generuje i pobiera wniosek o podpisanie certyfikatu usługi Apple Push Notification

2 Przejdź do Apple Push Certificates Portal

- Ta akcja przenosi Cię do portalu Apple Push Certificates

3 Importuj certyfikat Apple Push Notification service

- Ta akcja importuje plik certyfikatu serwisu Apple Push Notification z Twojego urządzenia

Apps and Books

Zaktualizowano: 3 cze 2026

Integracja Apps and Books umożliwia firmom i instytucjom zakup aplikacji i ich dystrybucję na urządzenia pracowników. Program umożliwia hurtowy zakup bezpłatnych i płatnych aplikacji. Przypisanie licencji aplikacji na urządzenie pozwala zainstalować aplikację bez konta iTunes.

Name: Start typing...

Organization: Start typing...

Expiration date: Select date

+

Reset filters

Selected: 1 | Deselect all

Add

☒	NAME	ORGANIZATION	DATE OF ADDING	EXPIRATION DATE	LAST SYNC DATE	
☒	Example	Proget Sp. z o.o.	2024-08-27 13:04:25	2025-04-25 14:17:59	2024-08-27 13:04:38	...

Results: 1 | Page limit: 50

<<

<

1

>

>>

1 Pokaż szczegóły

- Ta akcja pozwala na sprawdzenie szczegółów dodanej integracji Apps and Books, takich jak:
 - Jakie aplikacje są dodane do listy
 - Status wykorzystania licencji
 - Dostępność licencji na aplikacje

2 Edytuj

- Ta akcja pozwala na edytowanie danych dodanej integracji, takich jak:
 - Utwórz nową nazwę integracji
 - Dodaj nowy token Apps and Books

3 Synchronizuj licencje

- Ta akcja pozwala na synchronizację aktualnych informacji o licencjach

4 Usun

- Ta akcja pozwala na usunięcie integracji

5 Dodaj

- Ta akcja pozwala na dodanie nowych integracji
-

2 Dodaj konto Apps and Books

2.1 Nazwa

- Przykładowa nazwa dodanej integracji
- Wymagane

2.2 Token Apps and Books

- Wprowadź wygenerowany token Apps and Books
- Jak uzyskać token:
 - Zaloguj się na konto Volume Purchase Program (<https://business.apple.com>)
 - Zaloguj się na swoje konto
 - Wygeneruj token, a następnie wgraj go do systemu MDM
- Wymagane

2.3 Dodaj

- Ta akcja pozwala na dodanie pobranego tokena z Twojego urządzenia

2.4 Dodaj aplikacje macOS

- Jeśli zaznaczone, aplikacje iOS dostępne na macOS (Apple Silicon) zostaną również dodane do konsoli jako aplikacje macOS
-

3 Szczegóły konta Apps and Books

3.1 Pokaż zużycie licencji

- Ta akcja pozwala na sprawdzenie wykorzystania licencji
- Wówczas dowiesz się:
 - Które urządzenie wykorzystuje licencję
 - Który użytkownik korzysta z licencji

3.2 Wstecz

- Ta akcja pozwala na powrót do poprzedniego widoku

3.3 Lista integracji

- Lista integracji Apps and Books

Microsoft Entra ID Applications

Zaktualizowano: 3 cze 2026

Integracja z Microsoft Entra ID pozwala na powiązanie Proget z twoim Microsoft Entra ID. Dzięki temu dostępne będzie dodanie nowych połączeń umożliwiających import użytkowników do konsoli Proget.

Selected: 1 | Deselect all



Add

☒	NAME	CLIENT ID	TENANT ID	DATE ADDED	CLIENT SECRET EXPIRATION DATE
> ☒	Example name	00000000-0000-0000-0000-000000000000	00000000-0000-0000-0000-000000000000	2024-10-22 08:09:44	-

Results: 1 | Page limit: 50



1 Edytuj

- Ta akcja pozwala na edytowanie wybranej integracji

2 Synchronizuj

- Ta akcja pozwala na synchronizację wybranej integracji

3 Usuń

- Ta akcja pozwala na usunięcie wybranej integracji

4 Dodaj integrację Microsoft Entra ID

4.1 Nazwa

- Maksymalna długość tekstu to 255
- Wymagane

4.2 Client ID

- Client ID to unikalny identyfikator aplikacji (klienta) przypisany do twojej aplikacji przez Microsoft Entra ID, gdy aplikacja została zarejestrowana.
- Wymagane

4.3 Client Secret

- Client Secret to technika uwierzytelniania wykorzystująca wartość tekstową w aplikacji Microsoft zamiast certyfikatu do identyfikacji.
- Wymagane

4.4 Tenant ID

- Identyfikator dzierżawcy (Tenant ID) stanowi unikalny identyfikator lub alias dzierżawcy, który jest ustalany na podstawie nazwy dzierżawcy. Identyfikator ten jest przydzielany do zasobów dzierżawcy (takich jak koperty, mapy i dokumenty wychodzące).
- Wymagane

4.5 Ważność Client Secret

- Wybierz datę, kiedy Client Secret powinien wygasnąć

Samsung KME

Zaktualizowano: 3 cze 2026

Knox Mobile Enrollment to najszybszy i najbardziej zautomatyzowany sposób rejestracji dużej liczby urządzeń. Gdy administrator IT zarejestruje urządzenie w usłudze (przy użyciu numeru IMEI lub numeru seryjnego), użytkownik urządzenia inicjuje proces rejestracji MDM podczas początkowego procesu konfiguracji urządzenia.

* Customer ID:

00000000

* Region:

EU

Knox custom JSON:

1 Customer ID

- Wprowadź Customer ID
- Maksymalna długość tekstu to 255
- Wymagane

2 Region

- Wybierz region
- Jeden z
 - EU
 - US
- Wymagane

3 Knox custom JSON

- Wprowadź niestandardowe dane JSON

File Manager

Zaktualizowano: 3 cze 2026

BETA

Moduł umożliwia zarządzanie plikami na urządzeniach z systemem iOS oraz Android. Wymaga zainstalowanej i skonfigurowanej aplikacji File Manager. Dostępna przestrzeń na wgrane i pobrane pliki jest ograniczona - po jej przekroczeniu dalsze operacje na plikach nie będą możliwe. Aby odzyskać możliwość zarządzania plikami, należy usunąć wybrane pozycje z tabeli.

14%

Total capacity: 2.00 GiB (2.15 GB) Remaining capacity: 1.72 GiB (1.85 GB)

Files

Path: Start typing...

Vendor: Insert text here...

Model: Insert text here...

+

Reset filters

BASIC PQL

Selected: 0 | Deselect all

Download

Trash

Grid

Dropdown

☐	NAME	DIRECTORY	SIZE	USER	VENDOR	CREATION DATE	CREATED BY
☐	Gmail_2024.07.14.65324615...	/Directory	141.09 MiB ...	Example User	XIAOMI	2026-05-22 10:03:08	Example User
☐	Microsoft OneDrive_7.29_AP...	/Directory	99.29 MiB ...	Example User	XIAOMI	2026-05-22 10:02:50	Example User
☐	Android Auto_12.3.642634-r...	/Directory	43.19 MiB ...	Example User	XIAOMI	2026-05-22 10:00:07	Example User

1 Procent zapęłnienia dysku

- Wyświetla aktualny poziom wykorzystania przestrzeni dyskowej w postaci paska postępu z procentem zajętego miejsca, całkowitą pojemnością oraz pozostałą pojemnością

2 Filtr

- Filtr plików pozwala wyszukać dostępne pliki za pomocą podstawowych filtrów, takich jak:
 - Ścieżka
 - Producent
 - Model
 - Użyj przycisku '+', aby dodać dodatkowe kryteria filtrowania

3 Pobierz

- Ta akcja pozwala Ci pobrać zaznaczone pliki z listy na komputer
- Zaznacz jeden lub więcej plików z listy, aby aktywować tę akcję

4 Usun

- Ta akcja pozwala Ci usunąć zaznaczone pliki z przestrzeni File Manager, zwalniając miejsce na dysku
- Zaznacz jeden lub więcej plików z listy, aby aktywować tę akcję

5 Lista zaciągniętych plików

- Wyświetla wszystkie pliki zaciągnięte z urządzeń do przestrzeni File Manager, zawierające nazwę pliku, katalog, rozmiar, użytkownika, producenta urządzenia, datę utworzenia oraz użytkownika, który utworzył wpis

Changelog

Zaktualizowano: 6 lip 2026

× 2.20.4

2026-07-06

- Naprawiono reinstalację aplikacji w Proget Store

× 2.20.3

2026-06-29

- Naprawiono aktualizację aplikacji Apple za pomocą akcji

× 2.20.2

2026-06-26

- Zmieniono maksymalną liczbę znaków dla akcji 'Wyślij wiadomość'

× 2.20.1

2026-06-24

- Optymalizacje i inne usprawnienia

× 2.20.0

2026-06-16

- Dodano funkcjonalność File Manager - zdalne zarządzanie plikami na urządzeniach Android i iOS
- Dodano obsługę aplikacji Proget Notifier
- Dodano graf zależności (widok etykiety, karta użytkownika, karta urządzenia)
- Dodano zakładkę 'Dozwolone karty SIM'
- Dodano klucze PQL: device.SIM1, device.SIM2
- Dodano referencję PQL: ALLOWED_SIM_CARDS
- Dodano typ SCEP w profilu Certyfikat
- Dodano wgrywanie certyfikatów z pliku na urządzenia Windows
- Dodano nową akcję brak Internetu w profilu MTP

- Dodano opcjonalny numer telefonu i własny nagłówek w reakcji 'Zablokuj przestrzeń służbową' w profilu MTP
- Dodano generowanie raportu z błędów systemowych na urządzeniach Android
- Dodano masową edycję ustawień aplikacji w grupie
- Dodano aplikacje macOS w integracji Apps and Books
- Dodano zdalne usuwanie kont z urządzenia w zakładce 'Konta użytkowników'
- Dodano akcję 'Usuń konto Android Enterprise' w zakładce Urządzenia
- Dodano usuwanie integracji AE przy braku aktywnych kont na na urządzeniach z aktywacją Android Enterprise
- Dodano formatowanie tekstu i klikalne linki w wiadomościach do urządzenia
- Dodano kolumnę oczekujących akcji na listach
- Dodano stałą wysokość wierszy w tabelach
- Dodano opcje konfiguracji wyjścia z Kiosku
- Dodano opcje konfiguracji PIN w Kiosku
- Dodano ustawienia Proget w trybie pojedynczej aplikacji w Kiosku
- Dodano konfigurację pozycji Kiosku względem ekranu blokady
- Dodano konfigurację czasu automatycznego wylogowania w Kiosku
- Dodano nowe typy intentów w Kiosku: wylogowanie użytkownika, bezpośrednie wyjście z kiosku
- Zmieniono hasło serwisowe dla urządzeń Android - rozbudowa mechanizmu
- Zmieniono zachowanie custom atrybutów względem synchronizacji z Entra ID
- Oznaczono profil SCEP jako przestarzały
- Oznaczono politykę 'Hasło serwisowe' jako przestarzałą
- Oznaczono politykę 'Pozwalaj na czyszczenie danych aplikacji' jako przestarzałą
- Oznaczono kody zabezpieczeń dla urządzeń Android w Serwisie jako przestarzałe
- Naprawiono wyświetlanie adresu Wi-Fi MAC w zakładce Urządzenia

+ 2.19.12

2026-04-20

+ 2.19.11

2026-04-13

[+ 2.19.10](#)

2026-03-31

[+ 2.19.9](#)

2026-03-25

[+ 2.19.8](#)

2026-03-10

[+ 2.19.7](#)

2026-02-23

[+ 2.19.6](#)

2026-02-10

[+ 2.19.5](#)

2026-02-09

[+ 2.19.4](#)

2026-02-04

[+ 2.19.3](#)

2026-01-19

[+ 2.19.2](#)

2026-01-14

[+ 2.19.1](#)

2026-01-12

[+ 2.19.0](#)

2026-01-07

[+ 2.18.5](#)

2025-10-08

[+ 2.18.4](#)

2025-09-17

[+ 2.18.3](#)

2025-08-25

[+ 2.18.2](#)

2025-07-22

[+ 2.18.1](#)

2025-07-14

[+ 2.18.0](#)

2025-07-09

[+ 2.17.10](#)

2025-05-20

[+ 2.17.9](#)

2025-05-14

[+ 2.17.8](#)

2025-04-29

[+ 2.17.7](#)

2025-04-16

[+ 2.17.6](#)

2025-04-02

[+ 2.17.5](#)

2025-03-25

[+ 2.17.4](#)

2025-03-19

[+ 2.17.3](#)

2025-03-10

[+ 2.17.2](#)

2025-03-05

[+ 2.17.1](#)

2025-02-26

+ 2.17.0	2025-02-19
+ 2.16.4	2025-02-03
+ 2.16.3	2025-01-15
+ 2.16.2	2024-10-19
+ 2.16.1	2024-10-13
+ 2.16.0	2024-10-15
+ 2.15.10	2024-09-03
+ 2.15.9	2024-08-19
+ 2.15.8	2024-07-23
+ 2.15.7	2024-07-17
+ 2.15.6	2024-07-16
+ 2.15.5	2024-07-01
+ 2.15.4	2024-06-25
+ 2.15.3	2024-06-05

+ 2.15.2	2024-05-27
+ 2.15.1	2024-05-13
+ 2.15.0	2024-05-08
+ 2.14.5	2024-03-14
+ 2.14.4	2024-03-13
+ 2.14.3	2024-02-27
+ 2.14.2	2024-01-31
+ 2.14.1	2024-01-25
+ 2.14.0	2024-01-22
+ 2.13.4	2023-11-21
+ 2.13.3	2023-10-24
+ 2.13.2	2023-09-07
+ 2.13.1	2023-09-06
+ 2.13.0	2023-09-04

[+ 2.12.3](#)

2023-07-12

[+ 2.12.2](#)

2023-06-20

[+ 2.12.1](#)

2023-06-13

[+ 2.12.0](#)

2023-06-12

[+ 2.11.3](#)

2023-03-22

[+ 2.11.2](#)

2023-03-08

[+ 2.11.1](#)

2023-02-27

[+ 2.11.0](#)

2023-02-08

[+ 2.10.3](#)

2023-01-11

[+ 2.10.2](#)

2022-12-29

[+ 2.10.1](#)

2022-12-01

[+ 2.10.0](#)

2022-10-25

[+ 2.9.11](#)

2022-09-12

[+ 2.9.10](#)

2022-09-05

[+ 2.9.9](#)

2022-09-01

[+ 2.9.8](#)

2022-08-29

[+ 2.9.7](#)

2022-08-24

[+ 2.9.6](#)

2022-07-26

[+ 2.9.5](#)

2022-07-05

[+ 2.9.4](#)

2022-06-29

[+ 2.9.3](#)

2022-06-22

[+ 2.9.2](#)

2022-06-01

[+ 2.9.1](#)

2022-05-18

[+ 2.9.0](#)

2022-05-16

[+ 2.8.14](#)

2022-04-25

[+ 2.8.13](#)

2022-04-25

[+ 2.8.12](#)

2022-04-21

[+ 2.8.11](#)

2022-04-07

[+ 2.8.10](#)

2022-02-15

[+ 2.8.9](#)

2022-01-25

[+ 2.8.8](#)

2022-01-13

[+ 2.8.7](#)

2021-12-15

[+ 2.8.6](#)

2021-12-13

[+ 2.8.5](#)

2021-12-01

[+ 2.8.4](#)

2021-11-29

[+ 2.8.3](#)

2021-10-14

[+ 2.8.2](#)

2021-10-13

[+ 2.8.1](#)

2021-09-28

[+ 2.8.0](#)

2021-09-21

[+ 2.7.3](#)

2021-07-07

[+ 2.7.2](#)

2021-06-29

[+ 2.7.1](#)

2021-06-24

[+ 2.7.0](#)

2021-06-22

[+ 2.6.2](#)

2021-05-27

[+ 2.6.1](#)

2021-05-13

[+ 2.6.0](#)

2021-04-19

[+ 2.5.3](#)

2021-03-31

[+ 2.5.2](#)

2021-03-09

[+ 2.5.1](#)

2021-03-01

[+ 2.5.0](#)

2021-02-24

[+ 2.4.9](#)

2021-02-02

[+ 2.4.8](#)

2021-01-26

[+ 2.4.7](#)

2021-01-19

[+ 2.4.6](#)

2020-12-14

[+ 2.4.5](#)

2020-12-04

[+ 2.4.4](#)

2020-11-30

[+ 2.4.3](#)

2020-11-24

[+ 2.4.2](#)

2020-11-03

[+ 2.4.1](#)

2020-10-30

[+ 2.4.0](#)

2020-10-26

[+ 2.3.5](#)

2020-07-13

[+ 2.3.4](#)

2020-07-07

[+ 2.3.3](#)

2020-07-02

[+ 2.3.2](#)

2020-06-30

[+ 2.3.1](#)

2020-06-26

[+ 2.3.0](#)

2020-06-25

Znane problemy

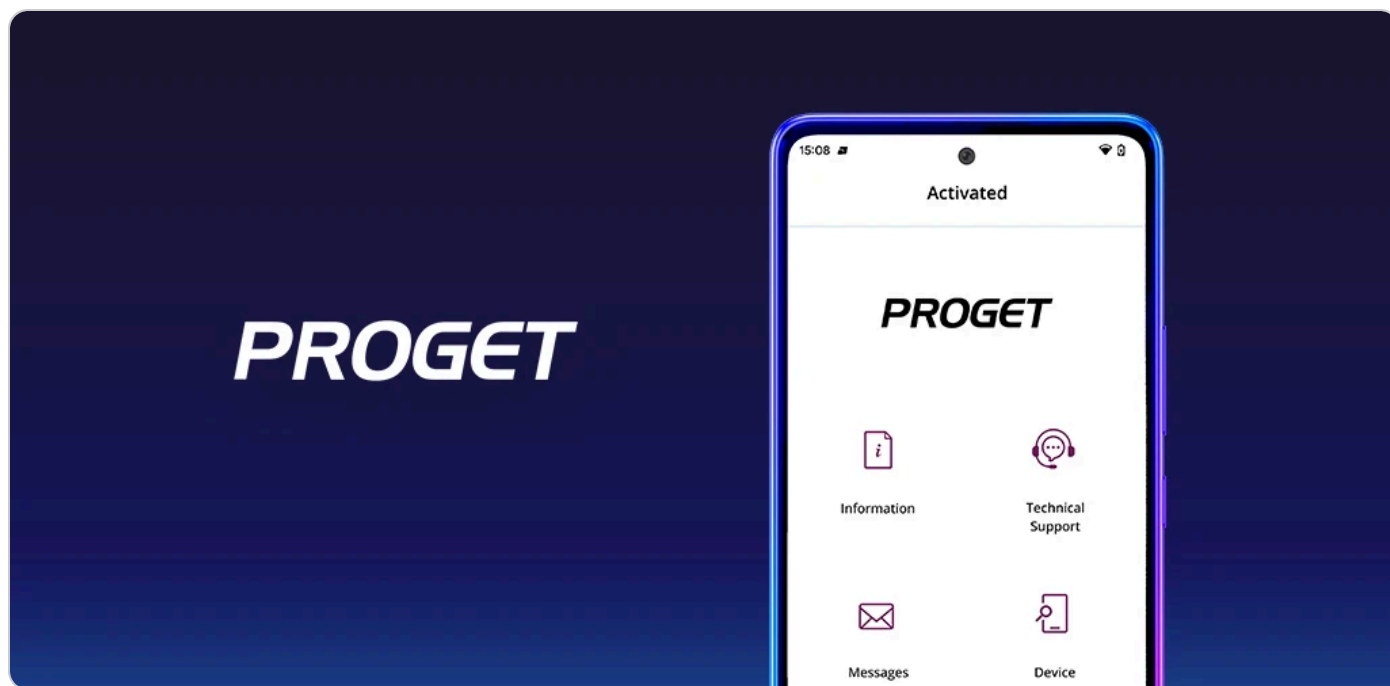
Zaktualizowano: 28 sty 2025

- + **Aplikacja e-mail Samsunga**
- + **Problem z uruchomieniem Remote Desktop**
- + **Strona Apple Business Manager nie jest dostępna**
- + **Urządzenie nie znika z karty użytkownika**
- + **Powtarzające się wystąpienia po przywróceniu kontaktów na Google Pixel (Device Owner)**
- + **Problem z synchronizacją przy aktywacji Windows**
- + **Polityka haseł przy aktywacji Windows**
- + **Tapeta profilu przy aktywacji iOS**
- + **Powiadomienia na urządzeniach Pixel z włączonym trybem Nie przeszkadzać**

Aplikacja mobilna Proget

Zaktualizowano: 4 mar 2025

Proget to rozwiązanie umożliwiające zarządzanie i administrowanie urządzeniami mobilnymi w firmie. Proget chroni firmowe i prywatne dane: pocztę e-mail, kalendarz, notatki i pliki dzięki funkcji wykonywania i przywracania kopii zapasowej kontaktów, sms/mms i rejestrów połączeń. Rozwiązanie zabezpiecza również mobilną transmisję danych z wykorzystaniem najwyższych standardów szyfrowania, tworząc bezpieczny tunel pomiędzy smartfonem a wewnętrznymi zasobami firmy. Proget umożliwia wdrożenie urządzeń w wielu modelach: BYOD, COPE lub urządzeń w pełni zarządzanych przez firmę.



[Changelog](#)



[Znane problemy](#)

Changelog

Zaktualizowano: 22 cze 2026

× 2.20.3

2026-06-22

- Naprawiono uprawnienia do SMS na aktywacji COPE

× 2.20.2

2026-06-12

- Naprawiono informowanie o zmianie karty SIM na urządzeniu
- Naprawiono ustawianie hasła na widoku Lost Mode
- Naprawiono działanie polityk automatycznej strefy czasowej, daty i godziny po restarcie urządzenia
- Inne poprawki i usprawnienia

× 2.20.1

2026-05-18

- Inne poprawki i usprawnienia

× 2.20.0

2026-05-12

- Ulepszono ustawienia Wi-Fi w profilu Kiosk
- Naprawiono łączenie się z siecią Wi-Fi WPA3 w ustawieniach w profilu Kiosk
- Naprawiono wyświetlanie notyfikacji o dostępie do danych użycia

+ 2.19.8

2026-04-21

+ 2.19.7

2026-03-26

+ 2.19.6

2026-03-25

+ 2.19.5

2026-03-02

+ 2.19.4

2026-02-03

+ 2.19.3

2026-01-19

+ 2.19.2

2026-01-12

+ 2.19.1

2025-12-02

+ 2.19.0

2025-11-27

+ 2.18.8

2025-10-20

+ 2.18.7

2025-09-10

+ 2.18.6

2025-08-19

+ 2.18.5

2025-08-14

+ 2.18.4

2025-08-06

+ 2.18.3

2025-07-29

+ 2.18.2

2025-07-16

+ 2.18.1	2025-07-15
+ 2.18.0	2025-06-30
+ 2.17.7	2025-05-20
+ 2.17.6	2025-04-14
+ 2.17.5	2025-04-06
+ 2.17.4	2025-04-02
+ 2.17.3	2025-03-24
+ 2.17.2	2025-02-27
+ 2.17.1	2025-02-21
+ 2.17.0	2025-02-10
+ 2.16.4	2025-01-27
+ 2.16.3	2025-01-08
+ 2.16.2	2024-12-10
+ 2.16.1	2024-11-28

+	2.16.0	2024-10-14
+	2.15.12	2024-09-02
+	2.15.11	2024-08-08
+	2.15.10	2024-08-07
+	2.15.9	2024-07-30
+	2.15.8	2024-07-03
+	2.15.7	2024-06-25
+	2.15.6	2024-06-14
+	2.15.5	2024-06-13
+	2.15.4	2024-05-20
+	2.15.3	2024-05-06
+	2.15.2	2024-05-02
+	2.15.1	2024-04-26
+	2.15.0	2024-04-25

[+ 2.14.3](#)

2024-03-27

[+ 2.14.2](#)

2024-03-12

[+ 2.14.1](#)

2024-01-25

[+ 2.14.0](#)

2024-01-15

[+ 2.13.5](#)

2023-11-28

[+ 2.13.4](#)

2023-11-07

[+ 2.13.3](#)

2023-10-17

[+ 2.13.2](#)

2023-09-04

[+ 2.13.1](#)

2023-08-25

[+ 2.13.0](#)

2023-08-23

[+ 2.12.0](#)

2023-06-05

[+ 2.11.1](#)

2023-02-28

[+ 2.11.0](#)

2023-02-20

[+ 2.10.3](#)

2022-11-25

[+ 2.10.2](#)

2022-10-27

[+ 2.10.1](#)

2022-10-26

[+ 2.10.0](#)

2022-10-25

[+ 2.9.3](#)

2022-07-07

[+ 2.9.2](#)

2022-06-22

[+ 2.9.1](#)

2022-05-27

[+ 2.9.0](#)

2022-05-16

[+ 2.8.10](#)

2022-02-24

[+ 2.8.9](#)

2022-01-20

[+ 2.8.8](#)

2022-01-19

[+ 2.8.7](#)

2022-01-03

[+ 2.8.6](#)

2021-12-02

[+ 2.8.5](#)

2021-11-30

[+ 2.8.4](#)

2021-11-08

[+ 2.8.3](#)

2021-11-03

[+ 2.8.2](#)

2021-10-13

[+ 2.8.1](#)

2021-10-04

[+ 2.8.0](#)

2021-09-21

[+ 2.7.6](#)

2021-09-01

[+ 2.7.5](#)

2021-07-11

[+ 2.7.4](#)

2021-07-07

[+ 2.7.3](#)

2021-07-06

[+ 2.7.2](#)

2021-06-24

[+ 2.7.1](#)

2021-06-22

[+ 2.7.0](#)

2021-06-22

[+ 2.6.4](#)

2021-05-12

[+ 2.6.3](#)

2021-05-07

[+ 2.6.2](#)

2021-04-27

[+ 2.6.1](#)

2021-04-21

[+ 2.6.0](#)

2021-04-19

[+ 2.5.4](#)

2021-03-16

[+ 2.5.3](#)

2021-03-04

[+ 2.5.2](#)

2021-03-03

[+ 2.5.1](#)

2021-03-01

[+ 2.5.0](#)

2021-02-19

[+ 2.4.11](#)

2021-01-25

[+ 2.4.10](#)

2021-01-11

[+ 2.4.9](#)

2021-01-04

[+ 2.4.8](#)

2020-12-29

[+ 2.4.7](#)

2020-12-21

[+ 2.4.6](#)

2020-12-09

[+ 2.4.5](#)

2020-11-27

[+ 2.4.4](#)

2020-11-26

[+ 2.4.3](#)

2020-11-25

[+ 2.4.2](#)

2020-11-20

[+ 2.4.1](#)

2020-10-30

[+ 2.4.0](#)

2020-10-26

[+ 2.3.6](#)

2020-08-21

[+ 2.3.5](#)

2020-08-11

[+ 2.3.4](#)

2020-07-03

[+ 2.3.3](#)

2020-06-30

[+ 2.3.2](#)

2020-06-26

[+ 2.3.1](#)

2020-06-25

[+ 2.3.0](#)

2020-06-25

Znane problemy

Zaktualizowano: 28 sty 2025

- + **Android Enterprise Device Owner – Polityka pozwalająca dodawać nowe połączenia Wi-Fi**
- + **Android Enterprise Device Owner – Instalacja aplikacji z pliku na urządzeniach Xiaomi**
- + **Android Enterprise Profile Owner – Samoistna zmiana haseł na urządzeniach Huawei z Androidem 8 lub 8.1**
- + **Android Enterprise – Device Owner na urządzeniach Nokia z Androidem 8**
- + **Uruchamianie aplikacji na urządzeniach HUAWEI**
- + **Nie można wybrać aplikacji Proget podczas przywracania wiadomości SMS/MMS w ramach aktywacji Android Profile Owner**
- + **Android Enterprise Profile Owner – obecnie niemożliwa jest przywrócenie kontaktów z kopii zapasowej na urządzeniach Huawei**
- + **Profil POP/IMAP nie działa z GMAIL**
- + **Xiaomi – niemożliwa instalacja aplikacji z pliku**
- + **HUAWEI EML-L29 Android 10 – Brak automatycznej rejestracji przy użyciu Enterprise QR**
- + **Xiaomi – interfejs MIUI**

+ Kontakt z administratorem i połączenie alarmowe na urządzeniach bez karty SIM

+ Akcja Wyłącz Wifi na profilu MTP

+ Wykonywanie zdjęć podczas Trybu Zagubionego na słabszych urządzeniach z Androidem

+ Polityka Dozwolone metody wprowadzania przy aktywacji DO i PO

+ Automatyczne ustawianie strefy czasowej – polityka DO na urządzeniach Samsung

+ Zabranianie usuwania dodanych sieci Wi-Fi – polityka DO na urządzeniach Samsung

+ Aktywacja Profile Owner poprzez QR z zakładki Integracja

+ Proget Backup – przywracanie MMS

+ Aktywacja DO poprzez Enterprise QR na Android 10

Aplikacja Proget Notifier

Zaktualizowano: 16 lip 2026

NOWOŚĆ

Aplikacja Proget Notifier to w pełni konfigurowalna warstwa komunikacji między konsolą zarządzania Proget a użytkownikiem urządzenia. Dzięki naszej aplikacji możesz wyświetlać na urządzeniu konfigurowalne ekrany z wiadomościami, obrazami i interaktywnymi przyciskami. Aplikacja obsługuje akcje takie jak wysyłanie danych na zewnętrzny endpoint, otwieranie dialera telefonicznego lub wyjście z aplikacji. Cała treść w tym teksty, obrazy i przyciski jest konfigurowalna per język i zarządzana zdalnie za pomocą konsoli zarządzania Proget. Aplikacja może również działać w trybie Kiosk jako pojedyncza aplikacja oraz zapewnia dostęp do ustawień Wi-Fi bezpośrednio ze swojego interfejsu. Ta aplikacja jest integralną częścią rozwiązania Proget. Zalecamy korzystanie z niej wyłącznie w środowisku zarządzanym przez system Proget.

PROGET
NOTIFIER



Changelog

Changelog

Zaktualizowano: 8 cze 2026

× 1.0.0	2026-05-28
Pierwsza wersja	

Aplikacja Proget File Manager

Zaktualizowano: 16 lip 2026

NOWOŚĆ

Aplikacja Proget File Manager umożliwia bezpieczny transfer plików między urządzeniami mobilnymi a konsolą zarządzania Proget. Dzięki naszej aplikacji możesz przysyłać pliki z urządzenia do konsoli i zarządzać nimi zdalnie. Dostępna przestrzeń dyskowa jest ograniczona po jej przekroczeniu dalsze operacje na plikach nie będą możliwe, dopóki wybrane pozycje nie zostaną usunięte. Ta aplikacja jest integralną częścią rozwiązania Proget. Zalecamy korzystanie z niej wyłącznie w środowisku zarządzanym przez system Proget. Aplikację można skonfigurować ręcznie lub zdalnie za pomocą konsoli zarządzania Proget.

PROGET
FILE MANAGER



Changelog

Changelog

Zaktualizowano: 16 lip 2026

× 0.1.1

2026-07-15

- Inne poprawki i usprawnienia

× 0.1.0

2026-06-29

- Pierwsza wersja

Aplikacja Proget Remote

Zaktualizowano: 4 mar 2025

Proget Remote to aplikacja, która umożliwia zdalny dostęp do ekranu urządzenia z systemem Android z serwera Proget. Bez względu na to, gdzie jesteś w danej chwili, nawiązując bezpieczne połączenie: uzyskaj szybką pomoc od administratora, napraw lub rozwiąż problem z urządzeniem, udostępnij ekran i przekaz kontrolę.



Changelog

Changelog

Zaktualizowano: 26 mar 2025

× **3.1.1**

2024-07-15

- Usprawniono stabilność połączenia

× **3.1.0**

2024-01-18

- Zmieniono UI aplikacji
- Dodano obsługę klawiatury podczas połączenia Proget Remote
- Dodano obsługę rotacji podczas połączenia Proget Remote

+ **3.0.1**

2023-11-07

+ **3.0.0**

2023-05-08

+ **2.4.4**

2022-02-07

+ **2.4.3**

2022-01-19

+ **2.4.2**

2021-10-21

+ **2.4.1**

2021-03-19

+ **2.4.0**

2021-03-18

+ **2.3.0**

2020-10-08

+ 2.2.0

2020-06-02

+ 2.0.0

2019-05-05

Aplikacja Proget Geofencing

Zaktualizowano: 4 mar 2025

Proget Geofencing to aplikacja, która pozwala zarządzać urządzeniem mobilnym w oparciu o wstępnie skonfigurowane strefy biznesowe. Dzięki niej administratorzy systemu Proget mają możliwość udostępniania różnych funkcjonalności i ograniczeń na urządzeniu mobilnym. Aplikacja nie działa samodzielnie. Do poprawnego działania Proget Geofencing konieczne jest użycie aplikacji Proget, która jest połączona z serwerem. Wymagana jest również dostarczona konfiguracja profilu Geofencing. Wszystkie konfiguracje i ograniczenia są w pełni konfigurowane przez administratora systemu Proget.



[Changelog](#)

Changelog

Zaktualizowano: 26 mar 2025

× **1.4.1**

2024-07-23

- Zmieniono UI aplikacji
- Naprawiono link do warunków korzystania

× **1.4.0**

2023-06-12

- Zmieniono UI aplikacji
- Poprawki błędów i inne usprawnienia

+ **1.3.1**

2021-03-26

+ **1.3.0**

2021-03-18

+ **1.2.0**

2020-10-09

+ **1.1.0**

2020-06-25

+ **1.0.0**

2019-12-04

Aplikacja Proget Backup

Zaktualizowano: 4 mar 2025

Proget Backup jest częścią systemu Proget. Może działać w trybie lokalnym (przeznaczonym wyłącznie do użytku osobistego) i zdalnym (przeznaczonym dla przedsiębiorstw). Użytkownik może tworzyć kopie zapasowe kontaktów, SMS-ów, MMS-ów, dzienników połączeń, a następnie przywracać je w razie potrzeby. Dane kopii zapasowej są bezpiecznie przechowywane w dedykowanej pamięci aplikacji. Aby korzystać z trybu zdalnego, aplikacja Proget musi być zarejestrowana na serwerze Proget. Aplikacja Proget Backup umożliwia administratorowi systemu Proget tworzenie i przywracanie kopii zapasowych kontaktów, SMS-ów, MMS-ów i rejestru połączeń. Wszystkie dane są pobierane i bezpiecznie przechowywane na serwerze Proget zarządzanym przez administratora w firmie.



**PROGET
BACKUP**



Changelog

Changelog

Zaktualizowano: 16 gru 2025

× 1.6.3

2025-12-15

- Naprawiono zaplanowane tworzenie kopii zapasowej po ponownym uruchomieniu aplikacji

× 1.6.2

2025-09-29

- Naprawiono ustawianie aplikacji Proget Backup jako domyślna aplikacja do SMS

× 1.6.1

2024-08-27

- Poprawki błędów i inne usprawnienia

× 1.6.0

2024-05-06

- Dodano możliwość wysłania kopii zapasowej na serwer bez rejestracji urządzenia w konsoli Proget

+ 1.5.0

2023-10-03

+ 1.4.3

2022-06-28

+ 1.4.2

2022-04-11

+ 1.4.1

2021-04-09

+ 1.4.0

2020-10-09

+ 1.3.0

2020-09-25

+ 1.2.0

2020-06-25

+ 1.1.0

2020-02-28

+ 1.0.0

2020-01-15

Aplikacja Proget File Sharing

Zaktualizowano: 4 mar 2025

Aplikacja Proget File Sharing zabezpiecza dostęp do zasobów firmowych poprzez FTP i SMB. Dzięki naszej aplikacji możesz uzyskać dostęp do zasobów firmowych przez FTP i SMB. Uzyskaj bezpieczny dostęp do danych firmowych i pracuj nad nimi zgodnie z zasadami obowiązującymi w Twojej organizacji. Ta aplikacja jest integralną częścią rozwiązania Proget. Zalecamy korzystanie z niej wyłącznie w środowisku zarządzanym przez system Proget. Aplikację można skonfigurować ręcznie lub zdalnie za pomocą konsoli zarządzania Proget.



Changelog

Changelog

Zaktualizowano: 26 mar 2025

× 1.5.1

2024-08-28

- Poprawki błędów i inne usprawnienia

× 1.5.0

2024-04-16

- Zmieniono UI aplikacji
- Dodano możliwość przesyłania plików z menedżera plików
- Dodano powiadomianie o błędzie podczas pobierania i przesyłania plików
- Naprawiono problem z konfiguracją zarządzaną
- Poprawki błędów i inne usprawnienia

+ 1.4.0

2023-07-05

+ 1.3.0

2021-12-13

+ 1.2.3

2021-09-23

+ 1.2.2

2021-08-31

+ 1.2.1

2021-05-12

+ 1.2.0

2021-05-07

+ 1.1.1

2021-04-02

+ 1.1.0

2021-03-31

+ 1.0.2

2021-03-18

+ 1.0.1

2021-03-15

+ 1.0.0

2021-03-05

Aplikacja Proget OpenVPN

Zaktualizowano: 4 mar 2025

Proget OpenVPN to aplikacja kliencka OpenVPN, która umożliwia ustanowienie bezpiecznego dostępu do poufnych danych za zaporą sieciową. Aplikacja obsługuje import profilu ovpn i zarządzaną konfigurację wysyłaną przez serwer EMM. Aby móc w pełni korzystać z rozwiązania, wymagane jest powiązanie aplikacji z serwerem EMM zainstalowanym w firmie lub w chmurze.

PROGET
OPENVPN



Changelog

Changelog

Zaktualizowano: 26 mar 2025

×	1.3.1	2024-01-17
	• Zaktualizowano UI aplikacji	
×	1.3.0	2024-01-16
	• Zmieniono UI aplikacji	
+	1.2.0	2023-06-29
+	1.1.2	2022-07-21
+	1.1.1	2022-07-15
+	1.1.0	2022-07-12
+	1.0.0	2022-01-21

FAQ

Zaktualizowano: 16 lip 2026

Co to jest MDM? (Mobile Device Management)

MDM – zarządzanie urządzeniami mobilnymi – to technologia zarządzania cyklem życia urządzenia umożliwiająca zespołowi IT wdrażanie, konfigurację, zarządzanie, obsługę i zabezpieczanie urządzeń mobilnych przez profile MDM zainstalowane na urządzeniach. Oprogramowanie MDM zapewnia zbiór zasobów, zdalną konfigurację poczty e-mail, aplikacji i WiFi, zdalne rozwiązywanie problemów oraz możliwość zdalnej blokady i wymazu w celu zabezpieczenia urządzenia i zgromadzonych na nim danych firmowych. MDM to podstawa kompleksowego rozwiązania do zarządzania mobilnością przedsiębiorstw (EMM, z ang. enterprise mobility management).

Czym jest MAM? (Mobile Application Management)

Technologie do MAM – zarządzanie aplikacjami mobilnymi – stosują kontrole zarządzania i zasad do poszczególnych aplikacji zamiast do całego urządzenia. Rozwiązania MAM zwykle oferują niestandardowy sklep z aplikacjami umożliwiający kontrolę i dostarczanie zarówno aplikacji opracowanych wewnętrznie, jak i aplikacji innych firm. Administratorzy IT mogą dodawać zabezpieczenia, szyfrowanie i kontrolę do aplikacji mobilnych, korzystając ze standardów AppConfig Community lub zestawu SDK (Software Development Kit) lub rozwiązań App Wrapping od dostawcy MAM.

Czym jest EMM? (Enterprise Mobility Management)

EMM – zarządzanie mobilnością przedsiębiorstw – to niezależne od urządzenia i platformy rozwiązanie centralizujące zarządzanie, konfigurację i zabezpieczenia wszystkich urządzeń w organizacji, zarówno tych używanych w modelu BYOD, jak i firmowych. EMM wykracza poza tradycyjne zarządzanie urządzeniami i obejmuje zarządzanie i konfigurację aplikacji i zawartości firmowej. Kompleksowe rozwiązanie EMM obejmuje MDM, MAM, MCM (mobile content management, czyli zarządzanie zawartością mobilną), zarządzanie tożsamością w celu kontroli dostępu oraz aplikacje produktywności w celu ułatwienia dostępu do firmowej poczty e-mail, kalendarza, kontaktów, repozytoriów zawartości i stron intranetowych. Dobrze dobrane rozwiązanie EMM powinno zapewnić zarówno możliwości techniczne umożliwiające uproszczenie zarządzania, jak i zabezpieczenia dla zespołu IT, a także przyjemne użytkowanie dla pracownika.

Czym jest UEM? (Unified Endpoint Management)

UEM – ujednolicone zarządzanie punktami końcowymi – pozwala zespołowi IT zaprzestać korzystania z odrębnych narzędzi do zarządzania urządzeniami mobilnymi, tradycyjnymi i IoT. Rozwiązania UEM zapewniają kompleksowe i skoncentrowane na użytkowniku podejście do zarządzania wszystkimi punktami końcowymi poprzez połączenie tradycyjnego zarządzania przez klienta komputerami stacjonarnymi i PC za pomocą nowoczesnej platformy zarządzania mobilnością przedsiębiorstw (EMM). Kompleksowe rozwiązanie UEM umożliwia zespołowi IT zarządzanie użytkownikami i dostarczanie spójnego doświadczenia na wszystkich punktach końcowych, zabezpieczanie i zarządzanie pełnym cyklem życia urządzenia i dokonanie tego wszystkiego z użyciem jednej kompleksowej platformy.

Czym jest BYOD? (Bring Your Own Device)

BYOD – zasada w branży IT pozwalająca pracownikom używać własnych urządzeń do celów służbowych. Platformy EMM umożliwiają organizacjom wdrożenie strategii BYOD bez narażenia bezpieczeństwa i prywatności pracowników na ryzyko, poprzez oddzielenie danych służbowych i osobistych na urządzeniu. Oddzielenie to pozwala zespołowi IT zarządzać i zabezpieczać tylko dane służbowe na urządzeniu będącym własnością pracownika. Jeśli urządzenie kiedykolwiek będzie zagrożone lub gdy pracownik odejdzie z firmy, zespół IT ma możliwość usunięcia tylko danych związanych z pracą i pozostawienia elementów osobistych na urządzeniu w nietkniętej postaci.

Z jakimi aplikacjami działają profile pocztowe?

Zablokowano wyświetlanie profilu **Active Sync** lub **IMAP / POP**, które są używane w aktywacji Samsung Knox będą wymagały aplikacji Samsung Mail. Jeśli chcemy skonfigurować profil pocztowy na aktywacjach Android Enterprise Profile Owner czy Android Enterprise Device Owner, możemy to zrobić poprzez [konfigurację aplikacji](#).

Co to jest tryb nadzorowany – iOS?

Tryb nadzorowany systemu iOS firmy Apple zapewnia administratorom więcej opcji podczas zarządzania urządzeniami firmy Apple, co jest przydatne w przypadku urządzeń należących do firmy wdrożonych na dużą skalę. Na przykład można ograniczyć funkcję AirDrop, uniemożliwić użytkownikom zmienianie nazwy urządzenia lub zastosować reguły aplikacji. Aby dodać urządzenie w trybie nadzorowanym należy skonfigurować profile Apple Business Manager lub użyć [Apple Configurator](#). Warto dodać, że dla iOS 11 i późniejszych urządzeń, konfiguracja profilu Apple Business Manager powinna być zawsze ustawiona domyślnie w trybie nadzorowanym.

Skąd się biorą aplikacje na liście aplikacji?

Po aktywacji urządzenia, do systemu dodawane są automatycznie aplikacje z urządzenia. Użytkownik również posiada możliwość [dodania aplikacji](#).

Jak uzyskać i korzystać z usługi Apple Business Manager?

Usługę Apple Business Manager można uzyskać poprzez dystrybutorów. Ich listę znajdziemy na [podanej stronie](#).

Szczegółowe informacje jak używać Apple Business Manager można znaleźć na [tej stronie](#).

Jakie systemy operacyjne urządzeń mobilnych wspieramy?

Zapewniamy wsparcie dla systemu Android 8.0 i nowszych, iOS 10.3 i nowszych oraz dla Windows 10.

Jakie porty w sieci należy odblokować, aby zadziałał pulpit zdalny?

443/TCP, 2222/TCP, 2222/UDP, 30000-59999/UDP – na urządzeniu i stronie komputera.