



Zarządzanie urządzeniami przenośnymi w przedsiębiorstwie

Korzyści związane z wdrożeniem nowych rozwiązań
w zakresie zarządzania

SPIS TREŚCI

1	Zarządzanie urządzeniami przenośnymi w firmie (ang. Enterprise Mobility Management (EMM))	2
2	Zatroszcz się o bezpieczeństwo urządzeń w sposób zautomatyzowany	4
2.1	Rejestracja mobilnych punktów końcowych	4
2.2	Inwentaryzacja urządzeń	7
2.3	Egzekwowanie bezpieczeństwa haseł	7
2.4	Zdalne blokowanie urządzenia i usuwanie znajdujących się na nim danych	8
2.5	Wykrywanie manipulacji	8
2.6	Aktualizacje oprogramowania sprzętowego	9
2.7	Blokowanie lub zatwierdzanie aplikacji	10
2.8	Konfiguracja aplikacji	11
2.9	Bezpieczeństwo dzięki certyfikatom, dystrybucji oprogramowania oraz korporacyjnej sieci Wi-Fi	11
2.10	Sprawdzanie zgodności z wytycznymi IT	11
2.11	Portal Self-Service – samodzielni użytkownicy	12
2.12	Program zakupów grupowych Apple Volume Purchase Program (VPP)	13
3	Kompleksowość, wydajność i prostota użytkowania	14
3.1	Rozwiązanie zintegrowane czy autonomiczne – która opcja będzie korzystniejszym wyborem dla Twojej firmy?	14
3.2	Nakład pracy związany z procesem wdrażania oraz użyteczność rozwiązań	14
3.3	Wyzwania związane z różnorodnością platform	14
3.4	Przejrzyste zarządzanie w czasie rzeczywistym	16
4	Lista kontrolna najważniejszych cech rozwiązania EMM	17
5	Podsumowanie	18

© 2025 baramundi software GmbH

Składane w niniejszym dokumencie oświadczenia dotyczące urządzeń i funkcjonalności technicznych nie są wiążące i służą wyłącznie celom informacyjnym.

Informacje podane w broszurze mogą ulec zmianie. DocID:WP-EMM-200903

Zarząd spółki baramundi: inż. (FH) Uwe Beikirch | Dr Lars Lippert

1 Zarządzanie urządzeniami przenośnymi w firmie (ang. Enterprise Mobility Management (EMM))

W dzisiejszych czasach korzystanie z urządzeń przenośnych jest standardową praktyką w wielu przedsiębiorstwach. Dostęp do danych firmowych z poziomu telefonu lub tabletu jest obecnie dla pracowników czymś oczywistym, wręcz oczekiwanym. Podczas gdy firmy czerpią korzyści płynące ze stosowania urządzeń przenośnych, informatycy powinni być świadomi zagrożeń związanych z ich wykorzystywaniem do celów zawodowych. Zanim laptopy, tablety i smartfony będą mogły zostać bezpiecznie zintegrowane z systemem IT firmy i staną się narzędziami codziennie użytkowanymi przez jej pracowników, konieczne jest wdrożenie skutecznych zabezpieczeń, jak na przykład zarządzania procesami inwentaryzacji.

Smartfony i tablety są obecnie równie częstym celem ataków cyberprzestępców, co tradycyjne komputery PC. W ostatnich latach systemy urządzeń przenośnych padały ofiarą licznych ataków cybernetycznych. Ekspert informują o pojawieniu się nowych rodzajów złośliwego oprogramowania. Firmy muszą wiedzieć, jak się przed nim bronić. Chcąc znaleźć rozwiązanie tego problemu, musimy najpierw zadać sobie pytanie:

- Jak bardzo skomplikowany jest proces integracji urządzeń z oprogramowaniem do ich zarządzania?
- Czy urządzenia przenośne mogą zostać poddane inwentaryzacji w systemie IT?
- Czy oprogramowanie do zarządzania urządzeniami przenośnymi pozwala członkom zespołu IT na ich konfigurację?
- Jakie rozwiązania z zakresu bezpieczeństwa powinno oferować tego rodzaju oprogramowanie?
- Czy rozwiązanie EMM obsługuje funkcjonalności właściwe dla konkretnych platform, tak, jak w przypadku usługi Apple Business Manager lub programu Android Enterprise?
- Rozwiązanie zintegrowane czy autonomiczne – która opcja będzie korzystniejszym wyborem dla firmy?
- Czy użytkowanie oprogramowania do zarządzania urządzeniami przenośnymi jest trudne i potencjalnie problematyczne?

Odpowiadając na te pytania, stworzysz krótką listę indywidualnych wymagań, które powinno spełnić oprogramowanie do zarządzania idealnie dopasowane do potrzeb Twojej firmy. Lista ta może posłużyć Ci za punkt wyjścia do przeprowadzenia bardziej szczegółowej oceny poszczególnych dostawców oprogramowania oraz wstępnej selekcji potencjalnych rozwiązań. Następnie, korzystając z powyższej listy wymagań, administratorzy IT zatrudnieni

w Twojej firmie powinni przetestować rozwiązanie EMM w praktyce i ponownie ocenić program. Cel wdrożenia oprogramowania do zarządzania urządzeniami przenośnymi jest taki sam, jak w przypadku komputerów PC: zapewnienie bezawaryjnej pracy urządzenia, monitorowanie jego statusu 24/7 oraz zagwarantowanie bezpieczeństwa sprzętu. Dzięki Enterprise Mobility Management, urządzenia mobilne mogą być odpowiednio zarządzane i chronione.

2 Zatroszcz się o bezpieczeństwo urządzeń w sposób zautomatyzowany

2.1 Rejestracja mobilnych punktów końcowych

Aby umożliwić zarządzanie urządzeniami przenośnymi za pośrednictwem rozwiązania EMM, muszą najpierw zostać wprowadzone do oprogramowania, a następnie zarejestrowane za pomocą serwera zarządzającego.

Można to zrobić na kilka sposobów:

- Rejestracja mobilnego punktu końcowego jako w pełni zarządzanego urządzenia korporacyjnego (urządzenie będące własnością firmy/wykorzystywane wyłącznie do celów zawodowych)
- Rejestracja mobilnego punktu końcowego jako urządzenia firmowego z możliwością korzystania do celów prywatnych (urządzenie będące własnością firmy/wykorzystywane do celów zawodowych i prywatnych)
- Rejestracja mobilnego punktu końcowego jako urządzenia prywatnego z dostępem do danych firmowych (korzystanie z prywatnego urządzenia do celów zawodowych)
- Rejestracja mobilnego punktu końcowego jako urządzenia dedykowanego (urządzenie firmowe przeznaczone do wykonywania określonego zadania)



Aktywacja urządzenia z systemem iOS przy pomocy DEP

2.1.1 Urządzenia firmowe wykorzystywane wyłącznie do celów zawodowych

Urządzenia firmowe wykorzystywane wyłącznie do celów zawodowych nie pozwalają użytkownikowi na korzystanie z urządzenia w celach innych niż biznesowe oraz, zgodnie z ich przeznaczeniem, nie zawierają żadnych danych osobowych. Sposób korzystania z tych urządzeń może zostać ograniczony przez specjalne wytyczne, uniemożliwiające lub przynajmniej utrudniające jakikolwiek „przypadkowe” użycie urządzenia do celów prywatnych. W ten sposób mobilny punkt końcowy jest dodatkowo zabezpieczony, jednak korzystanie z urządzenia może być niewygodne i przez to niechętnie użytkowane. W większości przypadków urządzenia tego typu leżą w szufladach biurka.

2.1.1.1 Program rejestracji urządzeń Apple (DEP)

Firma Apple umożliwia efektywne i szybkie włączenie urządzeń z iOS do systemu zarządzania urządzeniami przenośnymi za pomocą dedykowanego programu rejestracji urządzeń (ang. Device Enrollment Program (DEP)), będącego częścią Apple Business Managers.

Administrator IT może dostosować parametry tego procesu do indywidualnych potrzeb przedsiębiorstwa poprzez wprowadzenie niestandardowych konfiguracji, definiując poziomy uprawnień każdego z użytkowników urządzenia na etapie aktywacji mobilnego punktu końcowego.

Z punktu widzenia użytkowników końcowych, kluczową zaletą DEP jest szybsza i łatwiejsza aktywacja urządzenia w systemie zarządzania urządzeniami przenośnymi. Natomiast dla firmy największą zaletą tego rozwiązania jest zwiększony poziom bezpieczeństwa urządzeń: Administratorzy IT mogą być pewni, że urządzenia firmowe są stale zarządzane.

2.1.1.2 Proces wdrażania urządzeń z wykorzystaniem DEP

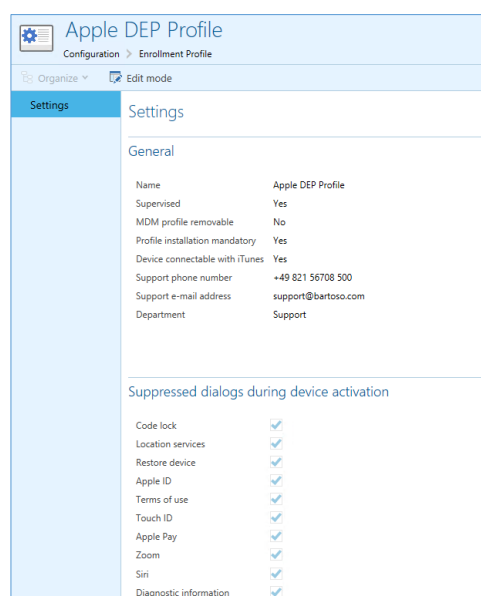
Przedstawione poniżej uproszczone procesy wdrożeniowe dla oprogramowania EMM są możliwe do przeprowadzenia dzięki wykorzystaniu rozwiązania DEP od Apple. DEP umożliwia znaczne skrócenie czasu wdrażania oraz inteligentną, masową rejestrację urządzeń. Użytkownicy końcowi otrzymują urządzenia z oryginalnym systemem operacyjnym, bezpośrednio połączone z systemem zarządzania.

2.1.1.3 DEP z perspektywy administratora IT

Administratorzy IT nie potrzebują fizycznego dostępu do urządzenia z systemem iOS, aby bezpiecznie zintegrować je z rozwiązaniem EMM.

Mają możliwość wstępnej konfiguracji nowego urządzenia za pomocą oprogramowania EMM, aby zapewnić zgodność z wytycznymi przedsiębiorstwa na etapie aktywacji punktu końcowego. W ten sposób mogą być pewni, iż wszystkie punkty końcowe zostały skonfigurowane w ten sam sposób i zawsze są monitorowane przez system do zarządzania urządzeniami przenośnymi.

Korzystając z prostej funkcji tworzenia profili, administratorzy mogą ustawić poziomy uprawnień użytkowników końcowych podczas aktywacji urządzenia.



Profil iOS do rejestracji urządzenia

2.1.2 Urządzenia firmowe z możliwością korzystania do celów prywatnych

Urządzenia firmowe z możliwością korzystania do celów prywatnych są własnością przedsiębiorstwa i są przekazywane pracownikom do użytku zarówno do celów zawodowych, jak i prywatnych. W związku z tym, wytyczne dotyczące sposobów korzystania z urządzenia są nieco mniej rygorystyczne, co zwiększa komfort użytkowania. Tego rodzaju sprzęt jest zazwyczaj zarządzany centralnie przez system zarządzania urządzeniami mobilnymi (ang. Mobile Device Management). Warto zauważyć, że w przypadku urządzeń służących celom zawodowym i prywatnym kluczowe znaczenie ma ochrona danych. Dane osobowe oraz aplikacje, z których użytkownik korzysta poza pracą powinny być zarządzane autonomicznie od danych i aplikacji firmowych. DEP może być stosowany – przy odpowiedniej konfiguracji – w przypadku urządzeń firmowych wykorzystywanych wyłącznie do celów zawodowych oraz urządzeń firmowych z możliwością korzystania do celów prywatnych.

2.1.3 Urządzenia prywatne z dostępem do danych firmowych (korzystanie z urządzenia osobistego do celów zawodowych)

Koncepcja Bring Your Own Device zakłada, iż podczas wykonywania obowiązków zawodowych pracownicy będą korzystać ze swoich własnych urządzeń. Podobnie jak w przypadku urządzeń firmowych z możliwością korzystania do celów prywatnych, na urządzeniu znajdują się zarówno dane osobowe, jak i firmowe. Rozdział tych dwóch grup danych jest w tym przypadku koniecznością. Istnieje również niebezpieczeństwo, że dane kontaktowe przedsiębiorstwa zostaną przeniesione do aplikacji, z których użytkownik korzysta w celach prywatnych, takich jak WhatsApp. Jednocześnie, administrator IT firmy nie może mieć dostępu do danych osobowych użytkownika urządzenia. Dlatego też idea Bring Your Own Device sprawdzi się tylko wtedy, gdy dane firmowe zostaną odseparowane od danych prywatnych, a obie grupy zostaną objęte odpowiednią ochroną. Dobrym rozwiązaniem problemu związanego z separacją danych jest wykorzystanie natywnych funkcji urządzeń z systemami iOS lub Android. Przykładowo: jeżeli użytkownik urządzenia podczas wykonywania obowiązków zawodowych korzysta z profilu służbowego Android Work Profile, administrator IT nie będzie miał dostępu do aplikacji, z których pracownik korzysta do celów prywatnych. W przypadku systemu iOS, na podobnej zasadzie działa funkcjonalność User Enrollment.

2.1.4 Urządzenia dedykowane

Firmowe urządzenia dedykowane są konfigurowane do wykonywania wyłącznie jednego konkretnego zadania; są to na przykład skanery kodów kreskowych lub urządzenia będące częścią systemów point-of-sale. W przypadku tego rodzaju urządzeń użytkownik nie ma dostępu do jakichkolwiek dodatkowych funkcjonalności ani nie może wykorzystywać go do innych celów. Może natomiast uruchomić tylko jedną aplikację – lub narzuconą z góry listę

aplikacji – zgodnie z regułami zdefiniowanymi przez administratora. Ponieważ urządzenia dedykowane obsługiwane są zazwyczaj przez większą liczbę użytkowników w całym przedsiębiorstwie, ich konfiguracja nie jest zależna od potrzeb jednego konkretnego użytkownika i nie wymaga jego identyfikacji.

2.2 Inwentaryzacja urządzeń

Które urządzenia są podpięte mojej sieci i jakie programy i aplikacje są na nich zainstalowane? Dobre oprogramowanie do zarządzania urządzeniami przenośnymi powinno być w stanie udzielić Ci podstawowych odpowiedzi na te pytania poprzez dostarczanie informacji na temat każdego urządzenia będącego częścią wspólnej platformy. Informacje o ustawieniach sprzętu i bezpieczeństwie, a także o zainstalowanych aplikacjach i uzyskanych certyfikatach mogą być zbierane dla urządzeń mobilnych z systemem iOS lub Android.

2.3 Egzekwowanie bezpieczeństwa haseł

Ochrona cennych danych firmowych przed nieautoryzowanym dostępem wymaga zabezpieczenia silnym hasłem. W przypadku urządzeń przenośnych, odpowiedni poziom bezpieczeństwa może zostać zagwarantowany poprzez zastosowanie rozwiązania EMM. Oprogramowanie do zarządzania urządzeniami przenośnymi umożliwia również określenie wymaganej złożoności haseł. Polityka szyfrowania urządzeń może być rozszerzona na urządzenia mobilne, które nie były wcześniej aktywowane. Oznacza to, że protokoły bezpieczeństwa mogą być wdrażane w sposób spójny i jednolity w całej organizacji.

Security policies

Common
iOS
Android
Windows Phone

General settings

Minimum password length

6

Password quality

complex

Password validity (days)*

30

Password history*

10

Display timeout (sec)

60

Password retries before device wipe

10

Encrypt internal storage*

☒

* on Android not before V3.0

Konfiguracja profilu bezpieczeństwa

2.4 Zdalne blokowanie urządzenia i usuwanie znajdujących się na nim danych

Ilekoć dane urządzenie zostanie zagubione, można je zdalnie zablokować i usunąć znajdujące się na nim dane. Jeśli użytkownik zapomni swojego hasła, administrator IT może udzielić mu pomocy w zdalnym odblokowaniu urządzenia. Urządzenie może zostać również zdalnie zablokowane – co uniemożliwia dalszy dostęp biometryczny do sprzętu – a odblokowanie może nastąpić tylko za pomocą kodu PIN określonego przez platformę obsługującą urządzenie. Tryb „zagubiony” pozwala administratorowi także na określenie lokalizacji urządzenia.

2.5 Wykrywanie manipulacji

Jeżeli mowa o modyfikacjach oprogramowania sprzętowego urządzeń mobilnych, dwa kluczowe pojęcia to Jailbreak (w przypadku urządzeń z systemem iOS) i Root (punkty końcowe z systemem Android). Modyfikacje te pozwalają użytkownikowi na instalowanie aplikacji z potencjalnie niepewnych źródeł, w tym alternatywnych sklepów z aplikacjami, lub na aktywowanie na urządzeniu funkcji, które nie zostały zweryfikowane lub zatwierdzone przez producenta. Instrukcje instalacji tego rodzaju modyfikacji można znaleźć w Internecie. Smartfony zmodyfikowane za pomocą Jailbreak lub Root niwelują zabezpieczenia systemu operacyjnego. To z kolei znacznie zwiększa ryzyko zainstalowania na urządzeniu złośliwego oprogramowania. W przypadku zmodyfikowanych urządzeń, oprogramowanie do zarządzania urządzeniami przenośnymi nie spełnia swoich zadań, ponieważ zabezpieczenia mogą być łatwo ominięte. Aby przeciwdziałać wyżej opisanym zagrożeniom, przedsiębiorstwa powinny stale obserwować i sprawdzać, czy do systemów operacyjnych nie zostały wprowadzone tego rodzaju modyfikacje.

Create new rule

Rule name: Jailbreak is not allowed

Severity: severe violation

Validation: ☒

Description: A manipulation of the firmware, a so-called jailbreak, was detected on your device. Please restore your device using an official firmware or contact your system administrator.

Execute job if rule is violated

Block Mail-Access on serverside
Send compliance issue to user

[Add job](#) | Remove job(s)

< Previous Create rule Cancel

Sprawdzanie, czy na urządzeniu nie zostało zainstalowane oprogramowanie Jailbreak

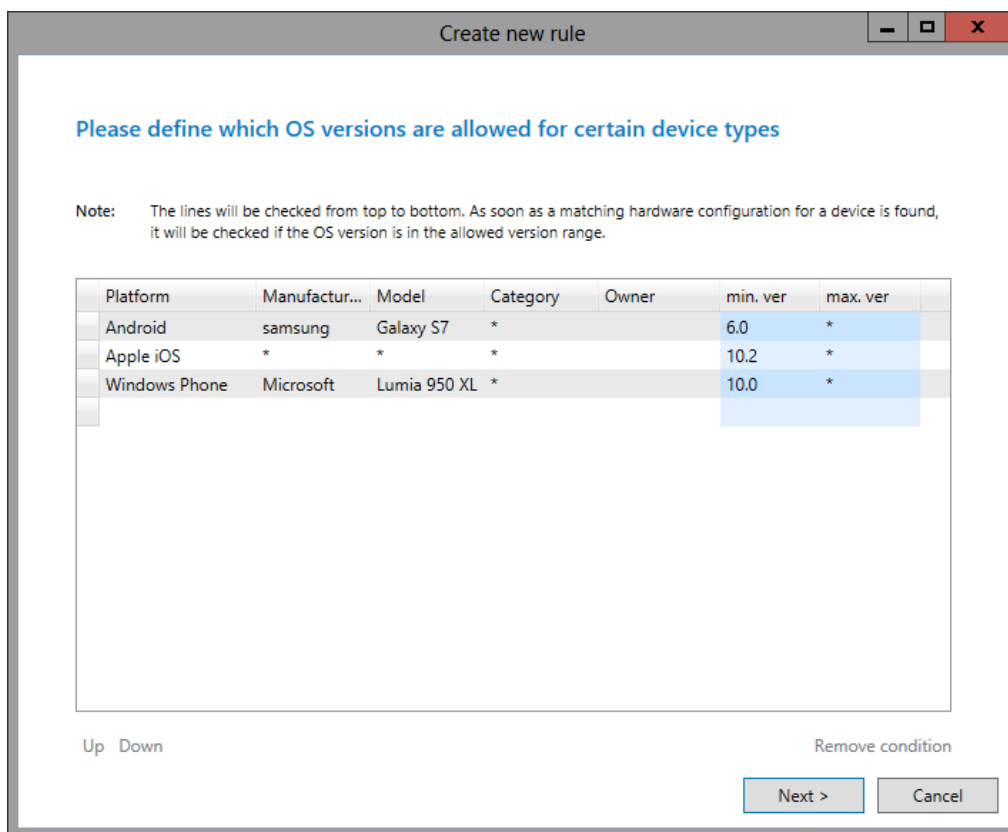
Urządzenia zmodyfikowane w ten sposób powinny być klasyfikowane jako urządzenia nieposiadające odpowiednich zabezpieczeń, a oprogramowanie EMM musi być w stanie rozpoznać tego rodzaju manipulacje. Wysokiej klasy oprogramowanie do zarządzania urządzeniami przenośnymi może reagować na nie automatycznie, na przykład poprzez ograniczanie dostępu zmodyfikowanych urządzeń do danych przedsiębiorstwa.

2.6 Aktualizacje oprogramowania sprzętowego

Aktualizowanie oprogramowania sprzętowego na bieżąco jest tak samo ważne jak zapobieganie wprowadzaniu do niego modyfikacji. Aktualizacje nie tylko wprowadzają do systemu nowe funkcje – eliminują również luki w zabezpieczeniach.

Zaawansowane rozwiązanie EMM ma znacznie większe możliwości niż tylko przeprowadzanie aktualizacji oprogramowania sprzętowego. Pozwala ono również administratorom na przeprowadzenie opóźnionych aktualizacji w określonych terminach (planowanie) oraz przetestowanie nowego oprogramowania sprzętowego i jego funkcji lub sprawdzenie bezpieczeństwa aplikacji firmowych opracowanych przez programistów na rzecz przedsiębiorstwa.

Monitorowanie wersji oprogramowania sprzętowego jest możliwe na wszystkich platformach. Dzięki inwentaryzacji urządzeń i automatycznemu testowaniu reguł oprogramowania administratorzy IT mogą w każdej chwili zdalnie uzyskać wgląd w dane urządzenie.



Create new rule

Please define which OS versions are allowed for certain device types

Note: The lines will be checked from top to bottom. As soon as a matching hardware configuration for a device is found, it will be checked if the OS version is in the allowed version range.

Platform	Manufactur...	Model	Category	Owner	min. ver	max. ver
Android	samsung	Galaxy S7	*		6.0	*
Apple iOS	*	*	*		10.2	*
Windows Phone	Microsoft	Lumia 950 XL	*		10.0	*

Up Down Remove condition

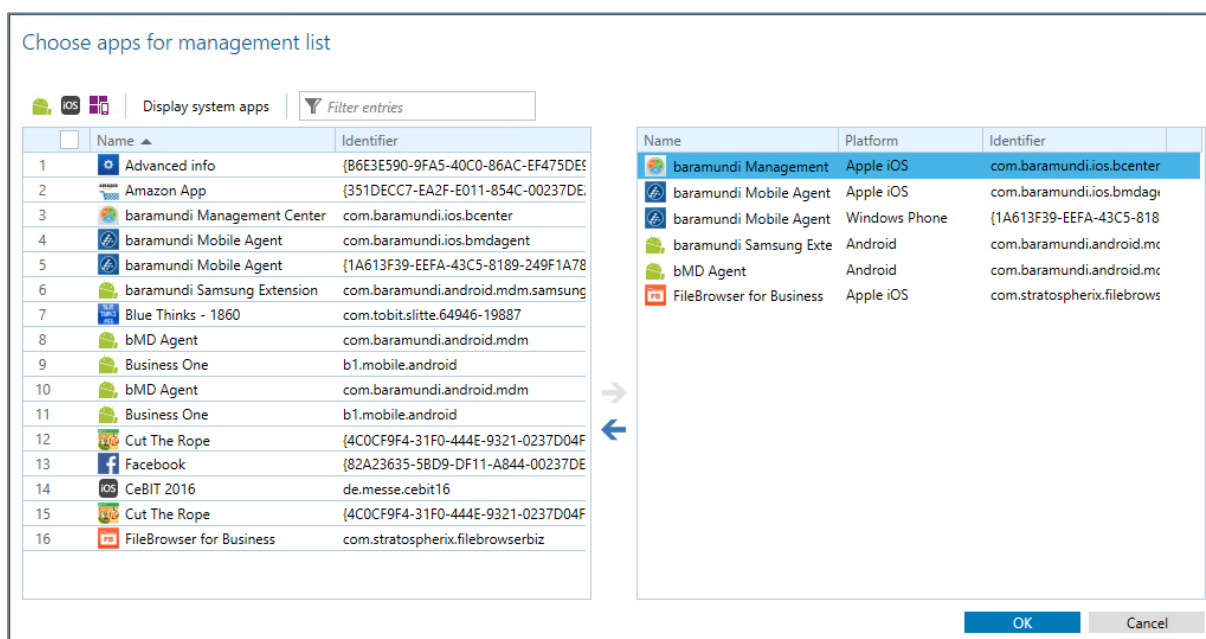
Next > Cancel

Testowanie reguł wersji systemu operacyjnego

2.7 Blokowanie lub zatwierdzanie aplikacji

Rozwiązanie EMM powinno umożliwiać blokowanie lub zatwierdzanie aplikacji. Przykładowo: oprogramowanie do zarządzania może zablokować instalację niepewnych lub niebezpiecznych aplikacji, jednocześnie umożliwiając użytkownikowi wyłącznie tych aplikacji, które zostały zatwierdzone przez przedsiębiorstwo i określone jako godne zaufania. W ten sposób administratorzy IT mogą zapobiegać instalowaniu lub używaniu niepożądanych aplikacji na urządzeniach przenośnych, którymi zarządzają. Z drugiej jednak strony, funkcja zatwierdzania aplikacji umożliwia administratorom określenie, które aplikacje będą dozwolone. Oznacza to, że każda aplikacja, która nie została zatwierdzona przez przedsiębiorstwo zostanie zablokowana podczas próby instalacji lub uruchamiania.

W zależności od przypadku, w danym urządzeniu można zarówno zatwierdzić, jak i zablokować konkretne aplikacje. Administratorzy IT, podjąwszy decyzję, którą z dwóch powyższych operacji wykonać, mają możliwość stworzenia listy dozwolonych aplikacji, a następnie zastosować ją w formie profili na dowolnym urządzeniu mobilnym.



Wybieranie oprogramowania do stworzenia listy zablokowanych/zatwierdzonych aplikacji

Dzięki EMM, administrator dostrzeże na pierwszy rzut oka, czy aplikacja zainstalowana fabrycznie może zostać bezpiecznie uruchomiona – nawet jeśli listy zablokowanych/zatwierdzonych aplikacji zostały stworzone w późniejszym terminie. Firma może korzystać z tych list, aby skutecznie bronić się przed niechcianymi i/lub niebezpiecznymi aplikacjami.

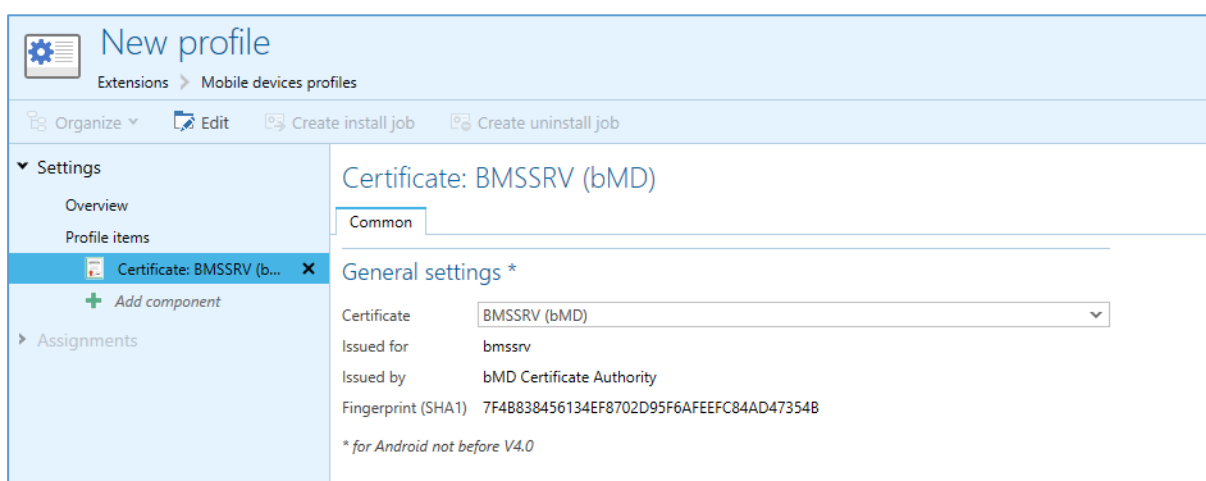
2.8 Konfiguracja aplikacji

Rozwiązanie Enterprise Mobility Management obejmuje wiele różnych aspektów zarządzania mobilnymi punktami końcowymi. Trzy najważniejsze obszary zastosowania tego rodzaju oprogramowania obejmują: Zarządzanie urządzeniami mobilnymi – Mobile Device Management (MDM), zarządzanie aplikacjami mobilnymi – Mobile Application Management (MAM) i zarządzanie treścią mobilną – Mobile Content Management (MCM). Obszary te obejmują zarządzanie całym urządzeniem, od aplikacji po treść mobilną na urządzeniu.

Poniższy schemat ilustruje zależności pomiędzy tymi trzema obszarami zarządzania z wykorzystaniem typowych mechanizmów.

2.9 Bezpieczeństwo dzięki certyfikatom, dystrybucji oprogramowania oraz korporacyjnej sieci Wi-Fi.

Rozwiązanie EMM powinno również wspierać dystrybucję certyfikatów klient-przedsiębiorstwo, gwarantując tym samym wzajemne zaufanie wymagane do utrzymania bezpieczeństwa usług świadczonych przez przedsiębiorstwo.



Struktura profilu dla certyfikatów klienta

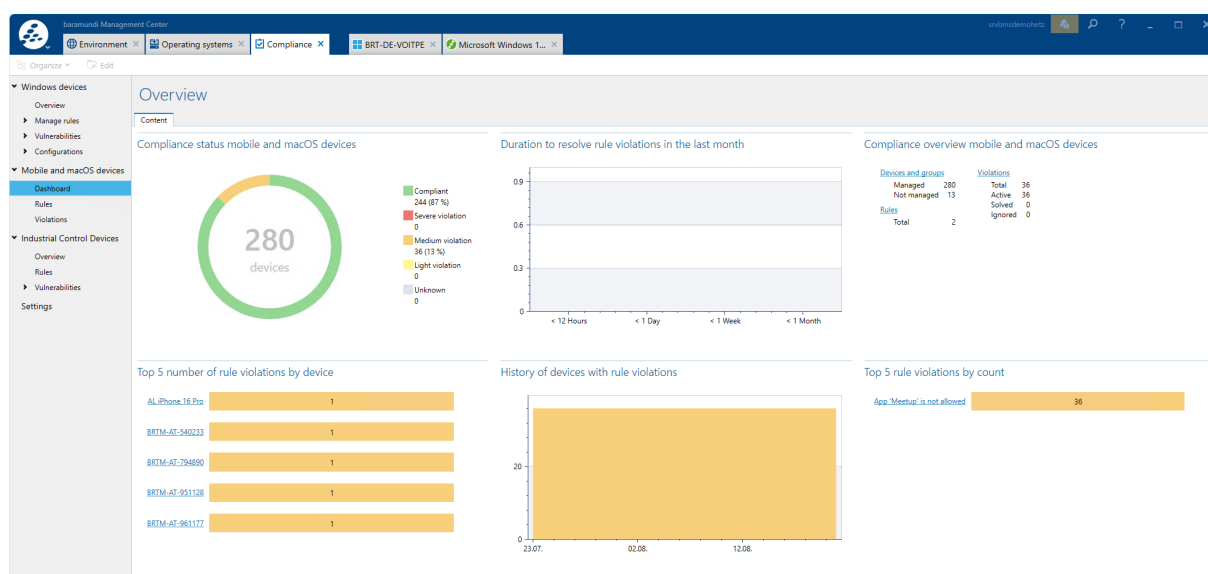
Korzystanie z takich certyfikatów może pomóc w zapewnieniu bezpiecznego dostępu przez Microsoft Exchange lub podczas wdrażania bezpiecznej sieci Wi-Fi w całym przedsiębiorstwie. W obu przypadkach bezpieczeństwo zależy od certyfikatów, a nie od loginów użytkowników.

2.10 Sprawdzanie zgodności z wytycznymi IT

Zapewnienie zgodności z zasadami przedsiębiorstwa jest szczególnie ważne w przypadku urządzeń mobilnych. Poza określeniem, które aplikacje zostaną umieszczone na liście aplikacji zablokowanych, a które na liście oprogramowania zatwierdzonego, a także

rozpoznaniem prób modyfikacji urządzenia, administratorzy mogą zidentyfikować i zainstalować wszelkie wymagane aplikacje, które mogą być nieobecne na danym urządzeniu.

Informacje o zgodności z zasadami przedsiębiorstwa powinny być wyraźnie widoczne na pulpitach nawigacyjnych użytkowników i uporządkowane według typu urządzenia i/lub stopnia ważności. Zapewnia to administratorom uproszczony przegląd informacji, ostrzegając ich o możliwych obszarach wymagających interwencji. Polecamy zakup rozwiązania EMM, które będzie obsługiwać automatyczne odpowiedzi – od powiadomień dla użytkowników wysyłanych za pośrednictwem poczty elektronicznej po zdalne usunięcie danych z urządzenia w przypadku poważnego naruszenia zasad narzuconych przez przedsiębiorstwo, takich jak instalacja oprogramowania Jailbreak na urządzeniu.



Pulpit nawigacyjny dla wytycznych IT

2.11 Portal Self-Service – samodzielni użytkownicy

Portal Self-Service to wygodne rozwiązanie dostarczane w ramach oprogramowania do zarządzania urządzeniami przenośnymi. Portal Self-Service udziela użytkownikom urządzeń mobilnych niezbędnego wsparcia, zmniejszając w ten sposób liczbę zapytań, którymi w innym przypadku musieliby zająć się informatycy. Gotowe do instalacji aplikacje i zadania mogą być dystrybuowane za pośrednictwem kiosku, bez konieczności angażowania administratora IT.

2.12 Program zakupów grupowych Apple Volume Purchase Program (VPP)

Firma Apple opracowała skierowany do przedsiębiorstw program zakupów grupowych, pozwalający na zakup i bieżące zarządzanie dystrybucją licencji na korzystanie z aplikacji, w tym również dodatkowymi opcjami użytkowania.

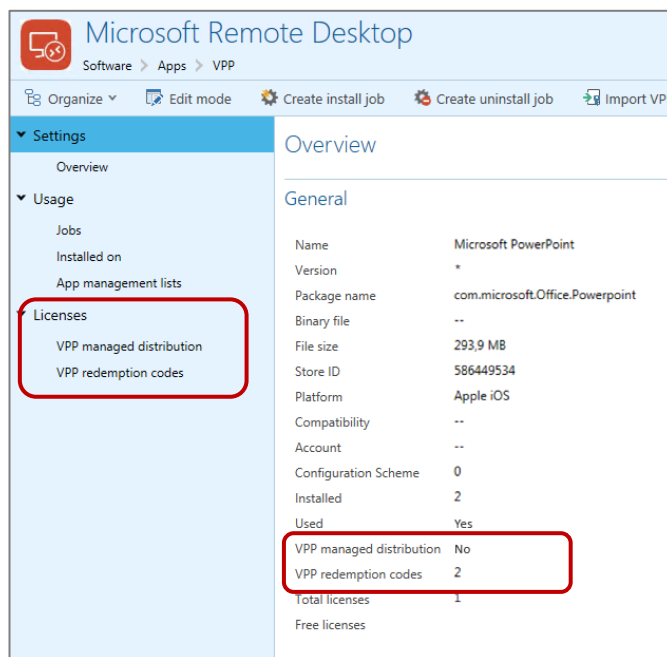
	Kody dostępu VPP	Zarządzanie dystrybucją aplikacji – dystrybucja na wszystkich urządzeniach użytkownika	Zarządzanie dystrybucją aplikacji – dystrybucja na wszystkich urządzeniach klienta
Powiązanie z licencjami	Apple ID*	Apple ID*	Urządzenie
Dystrybucja aplikacji	wyłącznie przez Apple ID*	wyłącznie przez Apple ID*	bez Apple ID*
Dystrybucja bez wchodzenia w interakcję z użytkownikiem	nie dotyczy	nie dotyczy	Tak (dla urządzeń nadzorowanych)
Obsługa licencji/wyświetlaczy za pomocą rozwiązania MDM	listy licencji; ręczne wprowadzanie danych	automatyczne powiązanie w oprogramowaniu MDM	automatyczne powiązanie w oprogramowaniu MDM
Administrator ma możliwość pozbawienia użytkownika licencji	nie dotyczy	tak	tak
Dostępny przez Apple	iOS 5	iOS 7	iOS 9

*) „Apple ID” odnosi się do identyfikatora użytkownika produktów/systemów Apple

2.12.1 Obsługa VPP z perspektywy administratora

Rozwiązanie VPP daje szerokie możliwości w zakresie dystrybucji płatnych lub darmowych aplikacji. Administratorzy mogą wybierać między korzystaniem z kodów dostępu do aplikacji a zarządzaniem dystrybucją indywidualnie dla każdej aplikacji.

Każda licencja przypisana do jednego urządzenia, może być również cofnięta i przeniesiona na inne urządzenie.



Obsługa VPP przez oprogramowanie baramundi Mobile Devices

3 Kompleksowość, wydajność i prostota użytkowania

3.1 Rozwiązanie zintegrowane czy autonomiczne – która opcja będzie korzystniejszym wyborem dla Twojej firmy?

Często dla decydentów w firmie sprawą kluczową jest kwestia, w jaki sposób rozwiązanie zostanie zintegrowane z istniejącym systemem informatycznym przedsiębiorstwa? Gdy firma zdecyduje się już na jedno z dostępnych na rynku rozwiązań w zakresie zarządzania urządzeniami przenośnymi, będzie mogła je zintegrować z systemem ujednoliconego zarządzania punktami końcowymi (ang. Unified Endpoint Management (UEM)) lub z autonomicznym rozwiązaniem EMM. Przedsiębiorstwa, które decydują się na wdrożenie UEM, mogą również zarządzać w ten sam sposób urządzeniami mobilnymi. Korzyści są wręcz oczywiste: Oprogramowanie do zarządzania urządzeniami przenośnymi zintegrowane z systemem ujednoliconego zarządzania punktami końcowymi umożliwia sprawowanie kontroli nad wszystkimi klientami za pomocą jednego interfejsu oraz zapewnia administratorom IT nieprzerwany dostęp do całego systemu. To rozwiązanie sprawdzi się idealnie w przypadku przedsiębiorstw zatrudniających niewielką liczbę administratorów odpowiedzialnych za infrastrukturę informatyczną, gdzie współdziałanie tych dwóch systemów może ułatwić ich pracę.

3.2 Nakład pracy związany z procesem wdrażania oraz użyteczność rozwiązań

Wybierając rozwiązanie z zakresu EMM, administratorzy powinni rozważyć, jak duży nakład pracy będzie wymagany do wdrożenia i uruchomienia oprogramowania oraz przeszkolenia pracowników. Integracja rozwiązania z istniejącą infrastrukturą IT powinna być możliwie jak najbardziej bezproblemowa. Należy również zastanowić się, czy rozwiązanie posiada przejrzysty interfejs, a jego obsługa jest intuicyjna. Powyższe warunki są niezbędne do spełnienia w celu zapewnienia, aby nowi pracownicy lub osoby zastępujące określonych pracowników szybko nauczyli się korzystać z oprogramowania EMM, eliminując tym samym potrzebę przeprowadzania szeroko zakrojonych szkoleń i ponoszenia dodatkowych kosztów. Pamiętajmy, że dla działów IT, których budżet jest napięty, aspekt finansowy jest naprawdę istotny.

3.3 Wyzwania związane z różnorodnością platform

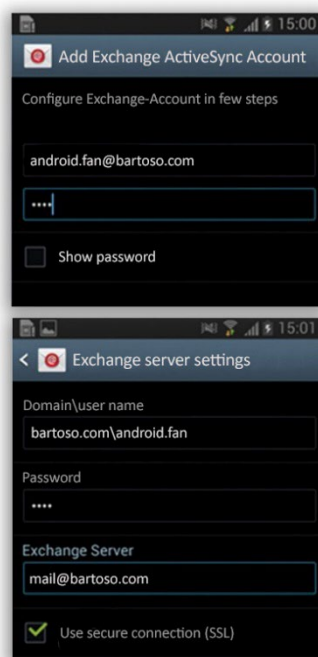
Administratorzy IT są często zmuszeni do obsługi wielu różnych platform mobilnych. Oznacza to, że muszą zrozumieć zasadę ich działania, być gotowym do wdrożenia każdej z platform, a

następnie zapewnienia wsparcia – w tym wprowadzenia wszystkich niezbędnych ustawień szczegółowych. Jest to nie tylko skomplikowane, ale i czasochłonne zadanie.

Przykładowo: podczas wprowadzania szczegółowych konfiguracji Exchange dla usługi e-mail dostarczanej przez dwie popularne platformy mobilne (Android i iOS), administratorzy muszą zazwyczaj określić podstawowe parametry (tj. nazwę, adres e-mail, domenę, serwer, szyfrowanie itd.) w osobnych oknach dialogowych.



iOS



Android

Konfiguracja Exchange na różnych platformach

To zrozumiałe, że wszyscy informatycy chcieliby móc korzystać z narzędzia, które zapewni spójność wprowadzanych danych we wszystkich zarządzanych urządzeniach. Dzięki zastosowaniu rozwiązania do zarządzania urządzeniami przenośnymi, administratorzy mogą korzystać z jednego interfejsu do ujednoliconego zarządzania wszystkimi urządzeniami mobilnymi. Przekłada się to na szybkie i sprawne wdrożenie konfiguracji Exchange, niezależnie od systemu operacyjnego.

Exchange account: Exchange

Common iOS Android Windows Phone

General settings *

Component name

Exchange

Display name on device

{RegisteredUser.Mail}

E-mail address

{RegisteredUser.Mail}

User name

{RegisteredUser.UserLogonName}

Domain

{RegisteredUser.Domain}

Exchange server (FQDN)

mail.bartoso.com

Encrypted communication

☒

Certificate selection

None

* for Android only supported by devices with Samsung KNOX or HTC Pro

Międzyplatformowa konfiguracja Exchange z wykorzystaniem oprogramowania do zarządzania urządzeniami przenośnymi

3.4 Przejrzyste zarządzanie w czasie rzeczywistym

Dobre rozwiązanie EMM dostarcza administratorom w czasie rzeczywistym aktualne i istotne dane dotyczące wszystkich zarządzanych urządzeń mobilnych. Ma to kluczowe znaczenie, ponieważ administratorzy będą w stanie prawidłowo ocenić bezpieczeństwo urządzeń mobilnych tylko wtedy, gdy posiadają pełen wgląd (w dowolnym momencie) we wszystkie niezbędne dane i informacje zwrotne. Nieograniczony dostęp do aktualnej bazy danych oznacza, że raporty są tworzone i opracowywane na bieżąco, w razie potrzeby.

4 Lista kontrolna najważniejszych cech rozwiązania EMM

Dystrybucja i konfiguracja oprogramowania	
☐	Dystrybucja Planowanie aktualizacji oprogramowania sprzętowego
☐	Możliwość odseparowania danych natywnych
☐	Instalacja aplikacji po potwierdzeniu bez potwierdzenia przez użytkownika
☐	Odinstalowanie aplikacji po potwierdzeniu bez potwierdzenia przez użytkownika
☐	Obsługa programu zakupów grupowych Apple Volume Purchase Program (VPP)
☐	Obsługa programu rejestracji urządzeń Apple Device Enrollment Program (DEP)
☐	Instalacja odinstalowanie z wyłączonym App Store
☐	Instalacja odinstalowanie własnych aplikacji przedsiębiorstwa
☐	Aplikacja Self-Service: Kiosk
☐	Instalacja odinstalowanie certyfikatów
☐	Parametryzacja ustawień z wykorzystaniem zmiennych
☐	Instalacja hiperłączy (iOS: Web Clip)
☐	Dezaktywacja kamery
☐	Konfiguracja punktów dostępowych (APN)
Inwentaryzacja urządzeń	
☐	Informacje o sprzęcie
☐	Skonfigurowane ograniczenia (blokada iCloud etc.)
☐	Zainstalowany profil
☐	Zainstalowany certyfikat
☐	Informacje na temat karty SIM
☐	Status roamingu
☐	Ustawienia bezpieczeństwa
☐	Ostatni kontakt
☐	Grupowanie urządzeń
Bezpieczeństwo	
☐	Zdalne blokowanie odblokowywanie urządzenia usuwanie danych z urządzenia
☐	Przypisanie PIN-u/podpowiedzi do hasła/złożoności hasła
☐	Wykrywanie manipulacji w zakresie oprogramowania sprzętowego (Jailbreak, Root)
☐	Określanie polityki szyfrowania urządzeń
☐	Możliwość tworzenia białej czarnej listy aplikacji
☐	Dezaktywacja aplikacji systemowych
☐	Dezaktywacja WLAN
☐	Dezaktywacja Bluetooth
☐	Historia hasła Reset Ustawianie nowego hasła
☐	Zezwolenie na dostęp / zablokowanie dostępu do karty SD
☐	Zezwolenie na dostęp / zablokowanie dostępu do sklepów z aplikacjami
☐	Automatyczne łączenie z siecią WLAN
Ocena zgodności	
☐	Wykrywanie faktu niezainstalowania istotnych aplikacji
☐	Wykrywanie faktu zainstalowania niepożądanych aplikacji
☐	Wykrywanie fałszywych konfiguracji
☐	Wykrywanie nieaktualnych wersji systemu operacyjnego
☐	Pokazywanie statusu i historii naruszenia reguł

5 Podsumowanie

Jeśli chodzi o wybór oprogramowania do zarządzania urządzeniami przenośnymi, nie ma jednego rozwiązania, które stanowiłoby odpowiedź na potrzeby wszystkich użytkowników. Ważne jest, aby jasno zdefiniować zestaw funkcji, które chcielibyśmy znaleźć w naszym oprogramowaniu i przetestować potencjalne rozwiązania. Poza oferowanymi funkcjami, kluczową rolę odgrywa również rodzaj przedsiębiorstwa, w którym wdrażane będzie oprogramowanie oraz planowany sposób wykorzystywania systemu. Poza stroną techniczną tego problemu, należy również wziąć pod uwagę potrzeby współpracowników i użytkowników końcowych. Jeżeli dane rozwiązanie EMM nie będzie spełniać ich wymagań, cały projekt w zakresie mobilności jest skazany na niepowodzenie. Z tego powodu, podejmując decyzję o wyborze oprogramowania do zarządzania urządzeniami przenośnymi, specjaliści do spraw IT powinni dążyć do osiągnięcia równowagi pomiędzy następującymi elementami:

- Wymagania przedsiębiorstwa dotyczące bezpieczeństwa
- Akceptacja rozwiązania dla urządzeń przenośnych przez współpracowników i użytkowników końcowych
- Bezproblemowe korzystanie z usług zarządzania urządzeniami mobilnymi przez przedsiębiorstwo za pośrednictwem zatrudnionych administratorów IT

Powodzenie jakiegokolwiek przedsięwzięcia z zakresu integracji oprogramowania EMM jest uzależnione od spełnienia wszystkich trzech powyższych wymagań.

baramundi software GmbH

Firma baramundi software rozwija zintegrowane zarządzanie punktami końcowymi do centralnego zarządzania komputerami, urządzeniami mobilnymi i serwerami. Automatyzuje dystrybucję oprogramowania, upraszcza zarządzanie poprawkami i zapewnia przejrzystość w sieci. baramundi wnosi w ten sposób znaczący wkład w bezpieczeństwo IT i redukuje zasoby.

www.baramundi.com

Czy jesteś gotowy, aby zapoznać się z naszym rozwiązaniem do zarządzania urządzeniami przenośnymi? Zapisz się na nasz webinar przeprowadzany na żywo!

Przekonaj się, jak zarządzać smartfonami i tabletami – bez wysiłku i niezawodnie, tak, jak w przypadku komputerów PC i laptopów!

www.baramundi.com/pl-pl/it-training/warsztaty-niestandardowe/

Czekamy na was!

Skontaktuj się z nami.



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

 +49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

 +48 735 91 44 54
request@baramundi.com
www.baramundi.com

 +49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

 +43 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

 +39 340 8861886
request@baramundi.com
www.baramundi.com

 +41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA

 +1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com