

Apress®

**Charles Edge**  
**Rich Trouton**

# **Zarządzanie urządzeniami Apple**

**Zunifikowana teoria zarządzania  
urządzeniami Mac, iPad, iPhone oraz  
AppleTV**

# Spis treści

Wstęp . . . . .	xiii
O autorach . . . . .	xviii
O recenzencie technicznym . . . . .	xviii
<b>Rozdział 1. Ewolucja zarządzania urządzeniami firmy Apple . . . . .</b>	<b>1</b>
Klasyczny system operacyjny Maców . . . . .	2
Protokoły sieciowe . . . . .	3
Wczesne zarządzanie urządzeniami . . . . .	5
NeXT . . . . .	8
Mac + Unix = Mac OS X . . . . .	10
Serwery . . . . .	14
Apple Remote Desktop . . . . .	20
Współistnienie ekosystemów . . . . .	22
Zarządzanie urządzeniami w iOS . . . . .	24
Zarządzanie urządzeniami mobilnymi . . . . .	26
Programy zarządzania urządzeniami Apple . . . . .	27
Mobilność korporacyjna . . . . .	29
iOS + Mac OS X = macOS . . . . .	32
tvOS . . . . .	33
Tworzenie obrazów zamarło? . . . . .	33
macOS – Unix = appleOS . . . . .	36
Odejście od Active Directory . . . . .	39
Społeczność administratorów Apple . . . . .	40
Konferencje . . . . .	41
Społeczności online . . . . .	42
Grupy użytkowników . . . . .	44
Podsumowanie . . . . .	45

<b>Rozdział 2. Zarządzanie oparte na agentach</b> . . . . .	<b>47</b>
<b>Demony i agenty</b> . . . . .	<b>48</b>
Użycie programu Lingon w celu łatwego przeglądania modyfikacji demonów i agentów . . .	51
Kontrolowanie demonów LaunchDaemon za pomocą launchctl. . . . .	54
<b>Dokładniejsza inspekcja: do czego ma dostęp aplikacja?</b> . . . . .	<b>56</b>
<b>Agenty zarządzania pochodzące od zewnętrznych podmiotów</b> . . . . .	<b>57</b>
Addigy . . . . .	58
FileWave. . . . .	61
Fleetsmith. . . . .	63
Jamf. . . . .	66
Munki. . . . .	69
osquery . . . . .	85
Chef . . . . .	93
Edycja przepisu . . . . .	96
Puppet . . . . .	98
<b>Użycie narzędzia git do zarządzania wszystkimi tymi rzeczami</b> . . . . .	<b>99</b>
<b>Wpływ UAMDM</b> . . . . .	<b>103</b>
<b>Rootless</b> . . . . .	<b>105</b>
<b>Frameworki</b> . . . . .	<b>106</b>
<b>Różne narzędzia do automatyzacji</b> . . . . .	<b>107</b>
<b>Podsumowanie</b> . . . . .	<b>109</b>
<b>Rozdział 3. Profile</b> . . . . .	<b>111</b>
<b>Ręczne konfigurowanie ustawień na urządzeniach</b> . . . . .	<b>112</b>
<b>Użycie narzędzia Apple Configurator do utworzenia profilu</b> . . . . .	<b>119</b>
Podglądanie nieprzetworzonej zawartości profilu . . . . .	128
Instalowanie profilu w systemie macOS . . . . .	131
Instalowanie profilu w systemie iOS . . . . .	134
Instalowanie profilu w systemie tvOS . . . . .	137
Podgląd profilu w systemie macOS. . . . .	141
Podgląd profilu w systemie iOS . . . . .	143
Podgląd profilu w systemie tvOS. . . . .	145
Usuwanie profilu w systemie macOS . . . . .	147
Usuwanie profilu w systemie iOS . . . . .	148
Usuwanie profilu w systemie tvOS . . . . .	150
Efekty usunięcia profilu . . . . .	152

<b>Użycie polecenia profiles w systemie macOS</b> .....	<b>153</b>
Użycie polecenia profiles .....	154
Rozszerzenia MCX dotyczące profili .....	156
<b>Podsumowanie</b> .....	<b>157</b>
<b>Rozdział 4. Wnętrze MDM</b> .....	<b>159</b>
<b>Do czego MDM może mieć dostęp</b> .....	<b>160</b>
<b>Apple Business Manager i Apple School Manager</b> .....	<b>161</b>
<b>Apple Push Notifications</b> .....	<b>166</b>
<b>Check-in: rejestracja urządzenia</b> .....	<b>167</b>
<b>MDM: zarządzanie urządzeniami</b> .....	<b>172</b>
<b>Polecenia MDM</b> .....	<b>174</b>
<b>Rejestracja automatyczna, czyli DEP</b> .....	<b>181</b>
API DEP dla dystrybutorów .....	182
API DEP usługi w chmurze .....	182
<b>mdmclient</b> .....	<b>185</b>
<b>Urządzenia nadzorowane</b> .....	<b>187</b>
<b>UAMDM</b> .....	<b>188</b>
<b>Polecenia rejestracji</b> .....	<b>191</b>
Wpływ UAMDM .....	192
<b>Włączanie rejestrowania w trybie debugowania APNs</b> .....	<b>203</b>
<b>Wdrażanie aplikacji</b> .....	<b>207</b>
Podarunki i kody VPP .....	208
Program zakupów grupowych (VPP) .....	209
<b>Zarządzanie otwieraniem</b> .....	<b>213</b>
<b>Hostowanie pliku .ipa na serwerze webowym</b> .....	<b>213</b>
<b>Podpisywanie oraz ponowne podpisywanie aplikacji dla systemu macOS</b> .....	<b>216</b>
Uwierzytelnianie notarialne aplikacji .....	216
<b>Podsumowanie</b> .....	<b>219</b>
<b>Rozdział 5. Wyposażanie systemu iOS</b> .....	<b>221</b>
<b>Wyposażanie systemu iOS</b> .....	<b>222</b>
Przygotowywanie urządzenia iOS za pomocą narzędzia Apple Configurator .....	223
Tworzenie Blueprints .....	223
<b>Zarządzanie zawartością</b> .....	<b>225</b>
Dodawanie certyfikatów dla 802.1x z profilami do Blueprint .....	225
Instalowanie aplikacji za pomocą narzędzia Apple Configurator .....	230

Automatyzacja rejestracji dzięki narzędziu Apple Configurator . . . . .	232
Zmiana nazwy urządzenia za pomocą narzędzia Apple Configurator . . . . .	237
Zmiana tapety za pomocą narzędzia Apple Configurator . . . . .	238
Przygotowywanie urządzenia . . . . .	240
Debugowanie z użyciem narzędzia Apple Configurator . . . . .	245
Użycie ipsw jako elementu przywracania urządzenia . . . . .	245
Nadzorowanie urządzeń za pomocą konfiguracji manualnej . . . . .	247
Automatyzacja działań w systemie iOS . . . . .	250
AEiOS . . . . .	261
<b>Usługi buforowania . . . . .</b>	<b>264</b>
Co jest buforowane? . . . . .	264
Konfigurowanie usługi buforowania . . . . .	265
<b>Podsumowanie . . . . .</b>	<b>270</b>
<b>Rozdział 6. Wyposażanie komputerów Mac . . . . .</b>	<b>271</b>
<b>Kombinacje klawiszy używane podczas uruchamiania systemu macOS . . . . .</b>	<b>272</b>
<b>Wyposażanie macOS z użyciem DEP . . . . .</b>	<b>273</b>
<b>Wyposażanie macOS bez użycia DEP . . . . .</b>	<b>276</b>
Instalacja . . . . .	276
Tworzenie przepływu . . . . .	277
Imagr . . . . .	284
Bootstrappr . . . . .	284
Installr . . . . .	284
Boot Camp . . . . .	285
Winclone . . . . .	285
<b>Upgrade’y i instalacje . . . . .</b>	<b>285</b>
Ponowne wyposażanie komputerów Mac . . . . .	288
Maszyny wirtualne . . . . .	292
<b>Podsumowanie . . . . .</b>	<b>293</b>
<b>Rozdział 7. Szyfrowanie urządzenia końcowego . . . . .</b>	<b>295</b>
<b>Przegląd szyfrowania w iOS . . . . .</b>	<b>295</b>
<b>Włączanie szyfrowania w systemie iOS . . . . .</b>	<b>298</b>
<b>Przegląd szyfrowania w macOS . . . . .</b>	<b>301</b>
<b>Secure Token . . . . .</b>	<b>303</b>
Włączanie szyfrowania w systemie macOS . . . . .	304
Klucze odzyskiwania FileVault . . . . .	307

FileVault 1 i plik FileVaultMaster.keychain . . . . .	308
Tworzenie instytucjonalnego klucza odzyskiwania . . . . .	310
Włączanie szyfrowania FileVault 2 dla jednego lub wielu użytkowników . . . . .	316
Włączanie szyfrowania FileVault 2 przy użyciu jednego lub wielu kluczy odzyskiwania . . . . .	325
Wyłączanie szyfrowania FileVault 2 . . . . .	329
Wyświetlenie listy aktualnych użytkowników FileVault 2 . . . . .	332
Zarządzanie indywidualnymi i instytucjonalnymi kluczami odzyskiwania . . . . .	333
Usuwanie indywidualnych i instytucjonalnych kluczy odzyskiwania . . . . .	337
Raportowanie dotyczące kluczy odzyskiwania . . . . .	340
Raportowanie statusu szyfrowania lub deszyfrowania za pomocą FileVault 2 . . . . .	343
<b>Podsumowanie . . . . .</b>	<b>346</b>
<b>Rozdział 8. Zabezpieczanie swojej floty . . . . .</b>	<b>347</b>
<b>Zabezpieczanie platformy . . . . .</b>	<b>348</b>
<b>Bezpieczeństwo komputerów Mac . . . . .</b>	<b>349</b>
Ochrona integralności systemu (SIP) . . . . .	350
Aplikacje chronione przez SIP . . . . .	352
Katalogi chronione przez SIP . . . . .	353
Interaktywne wyświetlanie zabezpieczeń SIP . . . . .	355
Ochrona w czasie wykonywania . . . . .	357
Ochrona rozszerzeń jądra . . . . .	358
<b>Zarządzanie SIP . . . . .</b>	<b>358</b>
NetBoot oraz SIP . . . . .	361
Uruchamianie csrutil poza środowiskiem Recovery . . . . .	363
Niestandardowe opcje konfiguracji SIP . . . . .	365
SIP i resetowanie NVRAM . . . . .	367
<b>Ochrona na poziomie użytkownika . . . . .</b>	<b>368</b>
<b>Wykrywanie typowych luk w zabezpieczeniach . . . . .</b>	<b>370</b>
<b>Zarządzanie zaporą macOS . . . . .</b>	<b>373</b>
<b>Zwalczanie złośliwego oprogramowania w systemie macOS . . . . .</b>	<b>375</b>
Xprotect oraz Gatekeeper . . . . .	375
<b>Isquarantine . . . . .</b>	<b>378</b>
Użycie Isregister do manipulowania bazą danych Launch Services . . . . .	380
Kwarantanna . . . . .	382
Zmianianie uchwytów plików . . . . .	383
MRT . . . . .	384

Podpisywanie aplikacji . . . . .	385
ClamAV . . . . .	386
<b>Zarządzanie zagrożeniami w systemie iOS . . . . .</b>	<b>388</b>
<b>Biała lista plików binarnych macOS . . . . .</b>	<b>390</b>
Zgodność . . . . .	392
Scentralizowane rejestrowanie i analiza dzienników . . . . .	393
Zapisywanie dzienników . . . . .	393
Odczytywanie dzienników . . . . .	394
Organizacja i klasyfikacja . . . . .	396
Porównania i wyszukiwania . . . . .	397
OpenBSM . . . . .	399
<b>Inżynieria odwrotna . . . . .</b>	<b>403</b>
<b>Podsumowanie . . . . .</b>	<b>407</b>
<b>Rozdział 9. Kultura automatyzacji i ciągłego testowania . . . . .</b>	<b>409</b>
<b>Skrypty i wiersz poleceń . . . . .</b>	<b>411</b>
<b>Podstawy wiersza poleceń . . . . .</b>	<b>412</b>
Podstawowe komendy powłoki . . . . .	414
<b>Skrypty powłoki . . . . .</b>	<b>418</b>
Deklarowanie zmiennych . . . . .	419
Interpretowanie w ZShell . . . . .	423
Dekorowanie zmiennych . . . . .	426
Standardowe strumienie i potoki . . . . .	429
Instrukcje if oraz case . . . . .	431
Instrukcje for, while i until . . . . .	436
Tablice . . . . .	439
Kody zakończenia . . . . .	440
Logika skryptów powłoki . . . . .	441
Testowanie ręczne . . . . .	449
Testy automatyczne . . . . .	451
Wysyłanie problemów do systemów zgłoszeniowych . . . . .	457
Symulowanie środowisk iOS za pomocą Xcode Simulator . . . . .	459
Corellium . . . . .	462
Orkiestracja API . . . . .	463
Zarządzanie wydaniem . . . . .	468
<b>Podsumowanie . . . . .</b>	<b>471</b>

<b>Rozdział 10. Usługi katalogowe</b> .....	<b>473</b>
<b>Ręczne dołączanie do Active Directory</b> .....	<b>474</b>
Najprostsze dowiązywanie .....	475
Dowiązanie przy użyciu Directory Utility .....	477
<b>Testowanie swojego połączenia za pomocą polecenia id</b> .....	<b>481</b>
<b>Użycie dscl do przeglądania katalogu</b> .....	<b>483</b>
<b>Programowe dowiązanie do usługi Active Directory</b> .....	<b>487</b>
<b>Dowiązanie do usługi Active Directory przy użyciu profilu</b> .....	<b>489</b>
Poza Active Directory .....	494
Wszystkie korzyści z dołączania bez dołączania .....	495
<b>Samodzielna aplikacja NoMAD</b> .....	<b>496</b>
<b>Profil konfiguracji</b> .....	<b>498</b>
NoMAD Login AD .....	501
<b>Apple Enterprise Connect</b> .....	<b>503</b>
<b>Podsumowanie</b> .....	<b>503</b>
<b>Rozdział 11. Dostosowywanie wrażeń użytkownika</b> .....	<b>505</b>
<b>Przekazywanie urządzeń z iOS i iPadOS w ręce użytkowników</b> .....	<b>506</b>
<b>macOS</b> .....	<b>507</b>
<b>Planowanie wrażeń użytkownika systemu macOS</b> .....	<b>507</b>
<b>Ochrona Transparency Consent and Control na folderach domowych użytkownika</b> ..	<b>508</b>
<b>Użycie profili do zarządzania ustawieniami użytkowników</b> .....	<b>509</b>
<b>Użycie skryptów do zarządzania ustawieniami użytkowników</b> .....	<b>513</b>
<b>Modyfikowanie domyślnego szablonu użytkownika systemu macOS</b> .....	<b>515</b>
Dostosowywanie pulpitu .....	516
Dostosowywanie preferencji użytkownika .....	517
<b>Konfigurowanie ekranu początkowego w iOS</b> .....	<b>517</b>
<b>Specjalne sklepy z apkami</b> .....	<b>519</b>
<b>Testowanie, testowanie, testowanie</b> .....	<b>521</b>
<b>Podsumowanie</b> .....	<b>522</b>
<b>Rozdział 12. Tożsamość i zaufane urządzenia</b> .....	<b>523</b>
<b>Użycie IdP dla tożsamości użytkowników</b> .....	<b>524</b>
<b>REST i uwierzytelnianie w sieci</b> .....	<b>525</b>
JSON .....	526
Użycie tokenów JWT jako kont usług .....	527



Tokeny na okaziciela . . . . .	529
<b>OAuth . . . . .</b>	<b>530</b>
<b>Webauthn . . . . .</b>	<b>533</b>
<b>OpenID Connect . . . . .</b>	<b>533</b>
SAML . . . . .	534
<b>Ciasteczka . . . . .</b>	<b>536</b>
<b>ASWebAuthSession . . . . .</b>	<b>538</b>
<b>Konfigurowanie testowego konta w Okta . . . . .</b>	<b>539</b>
Podgląd odpowiedzi SAML . . . . .	547
<b>Jamf Connect dla komputerów Mac . . . . .</b>	<b>548</b>
Konfigurowanie Jamf Connect Login . . . . .	549
<b>Jamf Connect dla systemu iOS . . . . .</b>	<b>553</b>
<b>Conditional Access . . . . .</b>	<b>556</b>
Konfigurowanie integracji Jamf z Intune . . . . .	557
<b>Poza uwierzytelnianiem . . . . .</b>	<b>562</b>
<b>Uwierzytelnianie wieloskładnikowe . . . . .</b>	<b>562</b>
Microsoft Authenticator . . . . .	563
MobileIron Access . . . . .	564
Conditional Access dla G-Suite . . . . .	565
<b>Duo Trusted Endpoints . . . . .</b>	<b>573</b>
<b>Managed Apple ID . . . . .</b>	<b>575</b>
Managed Apple ID w szkołach . . . . .	575
Managed Apple ID dla firm . . . . .	576
Użycie Managed Apple ID z Microsoft Azure Active Directory . . . . .	576
<b>Webhooki . . . . .</b>	<b>577</b>
<b>Praca z pękami kluczy . . . . .</b>	<b>580</b>
<b>Podsumowanie . . . . .</b>	<b>583</b>
<b>Rozdział 13. Przyszłość zarządzania urządzeniami firmy Apple . . . . .</b>	<b>585</b>
Zrównoważony arkusz ocen Apple . . . . .	586
Narzędzia . . . . .	589
Najbliższa przyszłość . . . . .	590
Kontrola prywatności . . . . .	591
Linie produktów firmy Apple . . . . .	592
Apki . . . . .	594
Ewolucja w projektach i architekturze oprogramowania . . . . .	594

Ewolucja oprogramowania Apple . . . . .	595
<b>Apki firmy Apple . . . . .</b>	<b>598</b>
Apki zarządzania . . . . .	598
Apki wydajności . . . . .	599
<b>Usługi firmy Apple . . . . .</b>	<b>599</b>
<b>Programy zarządzania urządzeniami firmy Apple . . . . .</b>	<b>602</b>
<b>Wprowadzanie apek na urządzenia . . . . .</b>	<b>603</b>
<b>Zarządzaj tylko tym czym musisz. . . . .</b>	<b>606</b>
<b>Przyszłość agentów . . . . .</b>	<b>607</b>
<b>Inne wpływy umieszczania w piaskownicach . . . . .</b>	<b>609</b>
<b>iOS, macOS, tvOS i watchOS pozostaną oddzielnymi systemami operacyjnymi . . . . .</b>	<b>610</b>
<b>Czy iOS stanie się naprawdę wieloużytkownikowy . . . . .</b>	<b>611</b>
<b>Zmiany w układach scalonych . . . . .</b>	<b>612</b>
<b>Jesteśmy firmą, a nie „przedsiębiorstwem” . . . . .</b>	<b>613</b>
<b>Apple jest firmą dbającą o prywatność . . . . .</b>	<b>614</b>
<b>Podsumowanie . . . . .</b>	<b>615</b>
<b>Dodatek A. Ekosystem Apple . . . . .</b>	<b>617</b>
Programy antywirusowe . . . . .	617
Narzędzia automatyzacji . . . . .	618
Kopie zapasowe . . . . .	619
Pakiety do współpracy i udostępnianie plików . . . . .	620
CRM . . . . .	621
Ekran powitalny DEP i menu pomocy . . . . .	621
Narzędzia programistyczne, środowiska IDE i manipulatory tekstu . . . . .	622
Digital Signage i kiosk . . . . .	624
Usługi katalogowe i narzędzia uwierzytelniania . . . . .	624
Zarządzanie tożsamością . . . . .	625
Narzędzia do konfigurowania i tworzenia obrazów . . . . .	625
Zbieranie i analizowanie dzienników . . . . .	626
Zestawy do zarządzania . . . . .	627
Różności . . . . .	629
Punkt sprzedaży . . . . .	629
Serwery wydruku . . . . .	629
Zdalne zarządzanie . . . . .	630
Narzędzia zabezpieczeń . . . . .	630

## Spis treści

Narzędzia pomocy technicznej . . . . .	631
Pakowanie oprogramowania i zarządzanie paczkami . . . . .	632
Przechowywanie plików . . . . .	633
Rozwiązywanie problemów, naprawa i narzędzia serwisowe . . . . .	634
Wirtualizacja i emulacja . . . . .	636
Rzeczy szczególnie istotne . . . . .	636
<b>Dodatek B. Typowe porty Apple . . . . .</b>	<b>637</b>
<b>Dodatek C. Zarządzanie NVRAM . . . . .</b>	<b>649</b>
<b>Dodatek D. Konferencje, pomocne grupy użytkowników i MacAdmins . . . . .</b>	<b>653</b>
<b>Indeks . . . . .</b>	<b>663</b>