

» Idź do

- Spis treści
- Przykładowy rozdział

» Katalog książek

- Katalog online
- Zamów drukowany katalog

» Twój koszyk

- Dodaj do koszyka

» Cennik i informacje

- Zamów informacje o nowościach
- Zamów cennik

» Czytelnia

- Fragmenty książek online

» Kontakt

Helion SA
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl
© Helion 1991-2008

Windows 7 PL. Księga eksperta

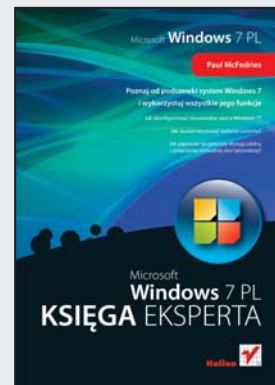
Autor: [Paul McFedries](#)

Tłumaczenie: Piotr Pilch, Julia Szajkowska,
Tomasz Walczak

ISBN: 978-83-246-2581-9

Tytuł oryginału: [Microsoft Windows 7 Unleashed](#)

Format: 172×245, stron: 920



Poznaj od podszewki system Windows 7 i wykorzystuj wszystkie jego funkcje

- Jak skonfigurować niezawodne sieci z Windows 7?
- Jak zautomatyzować zadania systemu?
- Jak zapewnić bezpieczny dostęp zdalny i połączenia wirtualnej sieci prywatnej?

doskonała znajomość Windows 7 PL pozwoli Ci optymalnie wykorzystać ten system. Masz przed sobą podręcznik napisany przez najwyższej klasy eksperta w tej dziedzinie, Paula McFedriesa, który prezentuje najbardziej skuteczne metody radzenia sobie ze wszystkimi problemami i zadaniami, począwszy od sieci i administrowania, a skończywszy na zabezpieczeniach i skryptach. Książka oferuje informatykom, a także wszystkim zaawansowanym i prawdziwym miłośnikom komputerów bogactwo potrzebnych im opisów ulepszeń, modyfikacji, technik i analiz związanych z systemem Windows 7.

Książka „Windows 7 PL. Księga eksperta” zawiera mnóstwo fachowych porad, sztuczek i metod diagnozowania systemu. W kolejnych rozdziałach omawiane są nowe metody dostrajania wydajności Windows 7, określania sposobu jego działania za pomocą zasad grupy czy modyfikowania rejestru. Korzystając z tego podręcznika, dowiesz się, jak zabezpieczyć system za pomocą usługi Windows Defender, oraz jak utworzyć sieć i zastosować komputer z Windows 7 w roli serwera. Poznasz także metody wykorzystywania najnowocześniejszych technik skryptowych, opartych na środowiskach Windows Scripting Host i Windows PowerShell.

- Wydajność i konserwacja systemu Windows
- Praktyczne metody przyspieszania ładowania systemu
- Edytor zasad grupy i edytor rejestru
- Konsola MMC i wiersz poleceń
- Zabezpieczenia systemu
- Funkcja automatycznego blokowania i blokowanie BitLocker
- Funkcja InPrivate
- Technologie sieciowe Windows 7
- Programowanie z zastosowaniem Windows Scripting Host i Windows PowerShell

Eksperska wiedza sprawi, że Windows 7 będzie Ci posłuszny!

Spis treści

O autorze	21
Wprowadzenie	23
Część I Dostosowywanie systemu Windows 7	29
Rozdział 1. Dostosowywanie programu Eksplorator Windows	31
Przywracanie menu w ich właściwe miejsce	32
Zmiana widoku	33
Wyświetlanie dodatkowych właściwości	34
Wyświetlanie rozszerzeń plików	36
Rezygnowanie z potwierdzania operacji usuwania	38
Uruchamianie Eksploratora Windows w trybie pełnoekranowym	41
Omówienie opcji widoku	41
Przenoszenie katalogów użytkownika	45
Przejmowanie prawa właściciela plików użytkownika	46
Wykonywanie niestandardowych operacji wyszukiwania	48
Zastosowanie funkcji Advanced Query Syntax do wyszukiwania właściwości	49
Zastosowanie zapytań w języku naturalnym	51
Rozdział 2. Dostosowywanie programu Internet Explorer	55
Wyświetlanie opcji internetowych	57
Kontrolowanie buforu stron WWW	57
Konfigurowanie historii stron WWW	59
Dodawanie wyszukiwarek do programu Internet Explorer	60
Użycie dowolnej wyszukiwarki z poziomu paska adresu	61
Zwiększanie efektywności kart	65
Wczytywanie wielu stron głównych podczas uruchamiania przeglądarki	66
Zaawansowane opcje programu Internet Explorer	68
Rozdział 3. Dostosowywanie systemu plików	77
Typy plików	78
Typy plików i ich rozszerzenia	79
Typy plików i rejestr	80
Praca z istniejącymi typami plików	82
Określanie domyślnej akcji	82
Tworzenie dla typu pliku nowej akcji	83
Przykład. Otwieranie okna interpretera poleceń dla bieżącego katalogu	85
Ukrywanie rozszerzenia typu pliku	86
Powiązanie rozszerzenia z inną aplikacją	87
Kojarzenie aplikacji z wieloma typami plików	89

Tworzenie nowego typu pliku	90
Powiązanie dwóch lub większej liczby rozszerzeń z pojedynczym typem pliku	91
Dostosowywanie nowego menu	91
Dodawanie typów plików do menu Nowy	92
Usuwanie typów plików z menu Nowy	93
Dostosowywanie okna dialogowego Otwieranie za pomocą systemu Windows 7	93
Otwieranie dokumentu przy użyciu nieskojarzonej aplikacji	94
Opis działania polecenia Otwórz za pomocą	95
Usuwanie dla typu pliku aplikacji z menu Otwórz za pomocą	96
Usuwanie programu z listy polecenia Otwórz za pomocą	96
Dodawanie programu do listy polecenia Otwórz za pomocą	97
Wyłączanie polecenia Otwórz za pomocą	97

Rozdział 4. Dostosowywanie procesów uruchamiania i zamykania 99

Dostosowywanie uruchamiania za pomocą danych konfiguracyjnych rozruchu	100
Użycie okna dialogowego Uruchamianie i odzyskiwanie do modyfikacji magazynu BCD	102
Zastosowanie narzędzia Konfiguracja systemu do modyfikacji magazynu BCD	103
Wykorzystanie narzędzia BCDEDIT do dostosowywania opcji uruchomieniowych	107
Dostosowywanie uruchamiania przy użyciu menu opcji zaawansowanych	111
Przydatne strategie logowania w systemie Windows 7	114
Logowanie w domenie	114
Włączanie konta Administrator	115
Konfigurowanie automatycznego logowania	117
Uniemożliwianie wyłączenia automatycznego logowania	119
Konfigurowanie operacji ponownego uruchamiania i zamykania wymagających jednego kliknięcia	119
Tworzenie skrótu polecenia restartowania systemu	122
Tworzenie skrótu polecenia zamykającego system	123
Wyłączanie z dowolnego miejsca komputera z systemem Windows 7	123
Dostosowywanie przycisku zasilania obecnego w menu Start	125
Dostosowywanie przycisków zasilania i uśpienia w komputerze przenośnym	126

Rozdział 5. Dostosowywanie menu Start i paska zadań 129

Dostosowywanie menu Start w celu łatwiejszego uruchamiania programów i otwierania dokumentów	131
Umieszczanie ulubionych programów w menu Start	131
Przypinanie na stałe ulubionego programu do menu Start	133
Czyszczenie zawartości listy niedawno używanych programów	135
Określanie domyślnych programów i dostępu do nich	136
Udoskonalanie menu Start przez zamianę odnośników na menu	137
Dodawanie, przenoszenie i usuwanie innych ikon menu Start	139
Dostosowywanie paska zadań w celu łatwiejszego uruchamiania programów i otwierania dokumentów	140
Zwiększanie wydajności za pomocą opcji paska zadań	140
Przypinanie ulubionego programu do paska zadań	143
Przypinanie lokalizacji docelowej do listy szybkiego dostępu	144

Użycie klawisza z logo systemu Windows do uruchamiania programów paska zadań	145
Kontrolowanie obszaru powiadomień	146
Wyświetlanie wielu zegarów dla różnych stref czasowych	149
Wyświetlanie wbudowanych pasków narzędzi paska zadań	151
Ustawianie wybranych opcji pasków narzędzi paska zadań	152
Tworzenie nowych pasków narzędzi paska zadań	152
Modyfikowanie menu Start i paska zadań za pomocą zasad grupy	152

Część II Wydajność i konserwacja systemu Windows 7155

Rozdział 6. Dostrajanie wydajności systemu Windows 7 157

Monitorowanie wydajności	158
Sprawdzanie klasyfikacji wydajności komputera	159
Monitorowanie wydajności za pomocą narzędzia Menedżer zadań	161
Zastosowanie narzędzia Monitor zasobów	165
Zastosowanie narzędzia Monitor wydajności	167
Optymalizowanie procesu uruchamiania	169
Ograniczanie lub eliminowanie testów wykonywanych przez BIOS	170
Zmniejszanie czasu oczekiwania dla menu opcji wyboru systemu operacyjnego	170
Rezygnowanie z ekranu powitalnego podczas uruchamiania systemu	171
Aktualizowanie sterowników urządzeń	171
Zastosowanie automatycznego logowania	171
Konfigurowanie wstępnego pobierania	172
Optymalizowanie aplikacji	172
Instalowanie dodatkowej pamięci	173
Instalowanie aplikacji na najszybszym dysku twardym	173
Optymalizowanie uruchamiania aplikacji	173
Uzyskiwanie najnowszych sterowników urządzeń	173
Optymalizowanie systemu Windows 7 pod kątem programów	174
Ustawianie priorytetu programu w oknie narzędzia Menedżer zadań	175
Optymalizowanie dysku twardego	176
Sprawdzanie parametrów wydajnościowych dysku twardego	176
Konserwacja dysku twardego	177
Wyłączanie kompresji i szyfrowania	177
Wyłączanie indeksowania zawartości	178
Uaktywnianie buforowania operacji zapisu	178
Konwertowanie partycji FAT16 i FAT32 na partycje NTFS	179
Rezygnowanie z tworzenia nazw plików w formacie 8.3	180
Rezygnowanie ze znacznika czasu ostatniej operacji dostępu	180
Optymalizowanie pamięci wirtualnej	181
Optymalne przechowywanie pliku stronicowania	181
Dzielenie pliku stronicowania	181
Dostosowywanie rozmiaru pliku stronicowania	182
Monitorowanie rozmiaru pliku stronicowania	183
Zmianie położenia i rozmiaru pliku stronicowania	183

Rozdział 7. Konserwacja systemu Windows 7	187
Sprawdzanie dysku twardego pod kątem błędów	188
Klasy	190
Cykle	191
Uruchamianie graficznego interfejsu narzędzia Sprawdź dysk	192
Sprawdzanie wolnej przestrzeni dyskowej	193
Usuwanie niepotrzebnych plików	196
Defragmentowanie dysku twardego	198
Uruchamianie narzędzia Defragmentator dysków	199
Zmiana harmonogramu narzędzia Defragmentator dysków	201
Wybieranie dysków przeznaczonych do defragmentacji	201
Przygotowanie na problemy	202
Tworzenie punktów przywracania systemu	203
Tworzenie dysku naprawy systemu	206
Sporządzanie kopii zapasowej plików	207
Konfigurowanie automatycznego sporządzania kopii zapasowej plików	209
Tworzenie kopii zapasowej obrazu systemu	212
Sprawdzanie dostępności aktualizacji i poprawek zabezpieczeń	213
Przeglądanie dzienników za pomocą narzędzia Podgląd zdarzeń	215
Tworzenie harmonogramu 9-krokowego procesu konserwacji	218
Część III Zaawansowane narzędzia systemu Windows 7	221
Rozdział 8. Kontrolowanie działania systemu Windows 7 z panelu sterowania	223
Wycieczka po panelu sterowania	224
Przegląd ikon panelu sterowania	226
Praca z plikami panelu sterowania	232
Prostszy dostęp do panelu sterowania	233
Alternatywne metody otwierania programów panelu sterowania	235
Panel sterowania w menu Start	236
Usuwanie ikon z panelu sterowania	237
Wyświetlanie określonych ikon panelu sterowania	238
Rozdział 9. Regulowanie pracy systemu Windows 7 za pomocą zasad grupy	241
Czym są zasady grupy?	242
Edytor lokalnych zasad grupy w różnych wydaniach systemu Windows	243
Uruchamianie edytora lokalnych zasad grupy	244
Tworzenie zasad grupy	245
Konfigurowanie zasady	246
Filtrowanie zasad	248
Przykładowe zasady grup	250
Personalizowanie okna zabezpieczeń Windows	251
Personalizowanie paska miejsc	253
Zwiększanie rozmiarów listy Niedawno używane elementy	255
Śledzenie zdarzeń zamknięcia systemu	256

Rozdział 10. Konfigurowanie konsoli Microsoft Management Console	259
Przegląd przystawek systemu Windows 7	260
Uruchamianie konsoli MMC	262
Dodawanie nowej przystawki	263
Zapisywanie stanu konsoli	265
Tworzenie nowego widoku bloku zadań	266
Operowanie przystawkami za pomocą zasad grupy	270
Rozdział 11. Zarządzanie usługami	273
Zarządzanie usługami za pomocą przystawki Usługi	274
Zarządzanie usługami za pomocą wiersza polecenia	277
Zarządzanie usługami za pomocą skryptów	278
Wyłączanie usług w celu usprawnienia pracy systemu	282
Szybsze zamykanie usług przez system Windows	286
Naprawianie uszkodzonej usługi	287
Rozdział 12. Poprawianie rejestru systemu Windows 7	291
Uruchamianie edytora rejestru	293
Pierwsze kroki w rejestrze	294
Poruszanie się w panelu kluczy	294
Czym są wartości rejestru?	295
Poznajowanie możliwości kluczy głównych rejestru	296
Czym są gałęzie i pliki rejestru?	298
Zapewnianie bezpieczeństwa rejestru	300
Zapobieganie wprowadzaniu zmian w rejestrze przez innych użytkowników	300
Wykonywanie kopii zapasowej rejestru	301
Zapisywanie bieżącego stanu rejestru za pomocą funkcji przywracania systemu	301
Eksportowanie kluczy rejestru do pliku na dysku	302
Wpisy w rejestrze	304
Zmianianie danych wpisanych w rejestrze	305
Zmiana nazwy klucza lub jego wartości	311
Tworzenie nowego klucza lub nowej wartości	311
Usuwanie klucza lub wartości klucza	312
Wyszukiwanie wpisów w rejestrze	312
Rozdział 13. Obsługiwanie systemu Windows 7 z wiersza polecenia	315
Uruchamianie wiersza polecenia	316
Uruchamianie wiersza polecenia z uprawnieniami administratora	317
Uruchamianie CMD	318
Praca w wierszu polecenia	322
Uruchamianie poleceń	322
Długie nazwy plików	323
Szybsze zmienianie katalogów	324
Wykorzystywanie narzędzia DOSKEY	325
Przekierowywanie poleceń do urządzeń wejścia i wyjścia	327
Polecenia potokujące	331

Podstawowe informacje o plikach wsadowych	332
Tworzenie pliku wsadowego	333
REM — dodawanie komentarzy w pliku wsadowym	333
ECHO — wyświetlanie wiadomości zawartych w pliku wsadowym	334
PAUSE — chwilowe wstrzymywanie wykonywania pliku wsadowego	335
Parametry w pliku wsadowym	336
FOR — pętle w pliku wsadowym	337
GOTO — przechodzenie do wskazanego wiersza pliku wsadowego	338
IF — warunki w plikach wsadowych	339
Narzędzia wiersza polecenia	343
Narzędzia zarządzania dyskiem	343
Narzędzia zarządzania plikami i katalogami	350
Narzędzia zarządzania pracą systemu	362

Część IV Bezpieczeństwo systemu Windows 7371

Rozdział 14. Zabezpieczanie systemu Windows 7 373

Powstrzymywanie szpiegów i crackerów	374
Najpierw podstawowe środki ostrożności	375
Blokowanie komputera	377
Wymaganie użycia kombinacji Ctrl+Alt+Delete przy uruchamianiu	379
Sprawdzanie ustawień zabezpieczeń komputera	380
Upewnianie się, że Zapora systemu Windows jest włączona	380
Upewnianie się, że program Windows Defender jest włączony	381
Upewnianie się, że kontrola konta użytkownika jest włączona	385
Upewnianie się, że konto administratora jest wyłączone	385
Zarządzanie Zaporą systemu Windows	386
Upewnianie się, że zaporę działa zgodnie z oczekiwaniami	387
Tworzenie wyjątków w Zaporze systemu Windows	387

Rozdział 15. Konfigurowanie zabezpieczeń w programie Internet Explorer 393

Zwiększanie prywatności w sieci WWW	395
Usuwanie historii przeglądania	395
Czyszczenie listy z paska adresu	399
Zwiększanie prywatności w internecie przez zarządzanie plikami cookies	402
Pełna prywatność — przeglądanie i filtrowanie InPrivate	405
Zwiększanie bezpieczeństwa w sieci WWW	406
Blokowanie wyskakujących okien	406
Dodawanie i usuwanie witryn w strefach	408
Zmianie poziomu zabezpieczeń dla strefy	410
Tryb chroniony — ograniczanie uprawnień Internet Explorera	411
Używanie filtra SmartScreen do powstrzymywania wyludzeń informacji	412
Kodowanie adresów w celu zapobiegania fałszowaniu nazw IDN	414
Zarządzanie dodatkami	416
Pełne bezpieczeństwo — Internet Explorer bez dodatków	417
Zaawansowane opcje zabezpieczeń w programie Internet Explorer	418

Rozdział 16. Zabezpieczanie poczty elektronicznej	421
Zabezpieczanie się przed wirusami w e-mailach	422
Konfigurowanie skanowania poczty elektronicznej w programie Windows Defender	426
Blokowanie niechcianych wiadomości za pomocą filtrów antyspamowych	
w Poczcie usługi Windows Live	427
Określanie poziomu ochrony przed niechcianą pocztą	428
Określanie bezpiecznych nadawców	430
Blokowanie nadawców	430
Blokowanie państw i języków	431
Zapobieganie wyłudzeniu informacji w e-mailach	432
Zapewnianie prywatności w czasie czytania e-maili	433
Blokowanie potwierdzeń	434
Blokowanie rysunków web beacon	434
Wysyłanie i otrzymywanie bezpiecznych e-maili	435
Konfigurowanie konta pocztowego z cyfrowym identyfikatorem	436
Pozyskiwanie klucza publicznego innej osoby	437
Wysyłanie bezpiecznych wiadomości	438
Odbieranie bezpiecznych wiadomości	439
Rozdział 17. Zabezpieczanie systemu plików	441
Ustawianie uprawnień do plików i folderów	442
Przypisywanie użytkownika do grupy	444
Przypisywanie użytkownika do wielu grup	445
Przypisywanie standardowych uprawnień	446
Przypisywanie uprawnień specjalnych	447
Szyfrowanie plików i folderów	449
Szyfrowanie dysku metodą BitLocker	451
Włączanie funkcji BitLocker w systemach z modułem TPM	452
Włączanie funkcji BitLocker w systemach bez modułu TPM	453
Rozdział 18. Konfigurowanie zabezpieczeń użytkowników	457
Wprowadzenie do kontroli konta użytkownika (KKU)	459
Podnoszenie uprawnień	460
Konfigurowanie kontroli konta użytkownika	462
Zasady kontroli konta użytkownika	464
Tworzenie bezpiecznych haseł i wymuszanie ich stosowania	466
Tworzenie silnych haseł	466
Ustawienia haseł kont użytkowników	467
Używanie zasad haseł w Windows 7	467
Przywracanie konta po zapomnieniu hasła	469
Tworzenie kont użytkowników i zarządzanie nimi	470
Używanie okna dialogowego Konta użytkowników	471
Ustawianie zasad dla kont	474
Ustawianie zasad związanych z zabezpieczeniami kont	475

Zarządzanie użytkownikami i grupami za pomocą wiersza polecenia	478
Polecenie NET USER	478
Polecenie NET LOCALGROUP	480
Stosowanie funkcji kontroli rodzicielskiej w celu ograniczenia możliwości korzystania z komputera	480
Aktywowanie kontroli rodzicielskiej	481
Przykład — konfigurowanie kontroli rodzicielskiej w obszarze gier	482
Inne sztuczki związane z zabezpieczeniami użytkowników	485
Zapobieganie podnoszeniu uprawnień przez wszystkich użytkowników standardowych	486
Blokowanie komputera przez wyłączenie kont wszystkich innych użytkowników	488
Ukrywanie nazw użytkowników na ekranie logowania	489
Zmianianie nazw wbudowanych kont w celu zwiększenia bezpieczeństwa	490
Używanie konta gościa do przyznawania użytkownikom tymczasowego dostępu do komputera	492
Określanie, kto jest zalogowany	492

Rozdział 19. Zabezpieczanie sieci 495

Zabezpieczanie sieci w Windows 7	496
Upewnianie się, że włączone jest udostępnianie chronione hasłem	497
Wyłączanie kreatora udostępniania	497
Ustawianie uprawnień udostępniania do folderów udostępnianych	499
Ustawianie uprawnień zabezpieczeń do folderów udostępnianych	501
Ukrywanie folderów udostępnianych	503
Wyłączanie ukrytych współużytkowanych udziałów administracyjnych	505
Usuwanie zapisanych poświadczeń pulpitu zdalnego	506
Blokowanie logowania w określonych godzinach	509
Określanie godzin logowania użytkownika	509
Automatyczne wylogowywanie użytkownika po upływie godzin logowania	510

Rozdział 20. Zwiększanie bezpieczeństwa sieci bezprzewodowej 513

Wyświetlanie stron konfiguracji routera	515
Wprowadzanie adresu IP routera	515
Korzystanie z okna Sieć	517
Ustawianie nowego hasła administratora	518
Umiejscawianie punktów dostępu pod kątem maksymalnego bezpieczeństwa	519
Szyfrowanie sygnałów w sieci bezprzewodowej za pomocą WPA	521
Zmianianie ustawień zabezpieczeń połączeń bezprzewodowych	523
Wyłączanie emisji sieciowego identyfikatora SSID	524
Łączenie się z ukrytą siecią bezprzewodową	525
Zmianianie domyślnego identyfikatora SSID	526
Włączanie filtrowania adresów MAC	528
Określanie adresów MAC bezprzewodowych kart sieciowych	529

Część V Rozwiązywanie problemów z systemem Windows 7531

Rozdział 21. Rozwiązywanie problemów i usuwanie skutków awarii systemu 533

Strategie rozwiązywania problemów — określanie przyczyn występowania problemu	535
Czy wyświetlił się komunikat o błędzie?	536
Czy komunikat o błędzie lub ostrzeżenie widnieje w oknie Podgląd zdarzeń?	537
Czy błąd jest widoczny w oknie Informacje o systemie?	537
Czy ostatnio edytowałeś wpisy w rejestrze?	538
Czy ostatnio zmieniałeś jakiegokolwiek ustawienia w systemie Windows?	538
Czy Windows 7 niekiedy wyłącza się i uruchamia?	538
Czy ostatnio zmieniałeś ustawienia którejś aplikacji?	541
Czy ostatnio zainstalowałeś na swoim komputerze nowy program?	543
Czy ostatnio podłączyłeś do komputera nowe urządzenie lub zainstalowałeś nowe sterowniki?	544
Czy ostatnio zainstalowałeś sterowniki niekompatybilne z systemem?	544
Czy ostatnio aktualizowałeś system, korzystając z usługi Windows Update?	544
Ogólne wskazówki dotyczące rozwiązywania problemów	545
Więcej narzędzi do rozwiązywania problemów	546
Narzędzia do rozwiązywania problemów zaimplementowane w systemie Windows 7	546
Diagnostyka dysku twardego	548
Wykrywanie wyczerpywania się zasobów systemowych	549
Narzędzie Diagnostyka pamięci systemu Windows	550
Wyszukiwanie rozwiązań problemów	551
Rozwiązywanie problemów z wykorzystaniem informacji znalezionych w sieci WWW	555
Przywracanie ustawień systemowych	556
Uruchamianie systemu w trybie ostatniej znanej dobrej konfiguracji	557
Naprawianie systemu za pomocą funkcji Przywracanie systemu	557

Rozdział 22. Rozwiązywanie problemów ze sprzętem 561

Zarządzanie urządzeniami za pomocą narzędzia Menedżer urządzeń	563
Różne sposoby wyświetlania urządzeń	564
Przeglądanie właściwości urządzenia	564
Wyświetlanie odłączonych urządzeń w Menedżerze urządzeń	565
Zarządzanie sterownikami	566
Konfigurowanie systemu Windows 7 tak, żeby ignorował brak podpisu cyfrowego sterowników	569
Tworzenie pliku tekstowego z pełną listą zainstalowanych sterowników urządzeń	573
Odinstalowywanie urządzeń	575
Zarządzanie zasadami bezpieczeństwa urządzeń	575
Rozwiązywanie problemów ze sprzętem	576
Rozwiązywanie problemów z użyciem Menedżera urządzeń	577
Wyświetlanie listy nie działających urządzeń	579
Rozwiązywanie problemów ze sterownikami urządzeń	582
Wskazówki dotyczące pobierania sterowników z sieci WWW	584
Rozwiązywanie problemów z nieprawidłowym współdzieleniem zasobów przez urządzenia	585

Rozdział 23. Rozwiązywanie problemów z uruchamianiem systemu 589

Zacznij od początku, czyli czynności, które należy wykonać, zanim zrobi się cokolwiek innego	590
Kiedy używać poszczególnych opcji uruchamiania?	592
Tryb awaryjny	592
Tryb awaryjny z obsługą sieci	592
Tryb awaryjny z wierszem polecenia	593
Włącz rejestrowanie rozruchu	593
Włącz wideo o niskiej rozdzielczości (640×480)	593
Ostatnia znana dobra konfiguracja (zaawansowane)	594
Tryb przywracania usług katalogowych	594
Tryb debugowania	594
Wyłącz automatyczne ponowne uruchamianie komputera po błędzie systemu	594
Opcja Wyłącz wymuszanie podpisów sterowników	594
Co zrobić, jeśli system nie chce uruchamiać się w trybie awaryjnym?	595
Przywracanie ustawień za pomocą funkcji odzyskiwania systemu	595
Rozwiązywanie problemów ze startem systemu za pomocą narzędzia Konfiguracja systemu	597

Część VI Technologie sieciowe systemu Windows 7601**Rozdział 24. Rozwiązywanie problemów z siecią 603**

Naprawianie połączenia sieciowego	604
Sprawdzanie stanu połączenia	606
Ogólne rozwiązania problemów z siecią	607
Włączanie odnajdowania sieci	608
Aktualizowanie firmware'u routera	610
Rozwiązywanie problemów z poziomu wiersza polecenia	612
Podstawowa procedura rozwiązywania problemów za pomocą wiersza polecenia	614
Badanie połączenia za pomocą polecenia PING	615
Śledzenie pakietów za pomocą polecenia TRACERT	617
Rozwiązywanie problemów z kablami	619
Rozwiązywanie problemów z kartą sieciową	620
Rozwiązywanie problemów z siecią bezprzewodową	621

Rozdział 25. Konfigurowanie małej sieci 623

Tworzenie sieci typu P2P	624
Zmianianie nazwy komputera i grupy roboczej	626
Nawiązywanie połączenia z siecią bezprzewodową	627
Używanie podstawowych narzędzi i wykonywanie zadań związanych z siecią w Windows 7	629
Otwieranie Centrum sieci i udostępniania	630
Tworzenie grupy domowej	632
Wyłączanie połączeń z grupą domową	636
Wyświetlanie komputerów i urządzeń dostępnych w sieci	636
Wyświetlanie mapy sieci	638
Wyświetlanie szczegółowych informacji o stanie sieci	639
Dostosowywanie ustawień sieci	641

Zarządzanie połączeniami sieciowymi	642
Otwieranie okna połączeń sieciowych	643
Zmianianie nazw połączeń sieciowych	644
Włączanie automatycznego przypisywania adresów IP	644
Ustawianie statycznego adresu IP	647
Sprawdzanie adresu MAC połączenia	651
Używanie połączenia sieciowego do wznawiania działania komputera w stanie uśpienia	652
Wyłączanie połączenia sieciowego	655
Zarządzanie połączeniami z siecią bezprzewodową	655
Otwieranie okna Zarządzaj sieciami bezprzewodowymi	656
Tworzenie sieci bezprzewodowych typu ad hoc	656
Zarządzanie właściwościami połączenia bezprzewodowego	659
Zmianianie nazw połączeń bezprzewodowych	661
Zmianianie kolejności połączeń bezprzewodowych	662
Tworzenie połączeń bezprzewodowych specyficznych dla użytkownika	663
Usuwanie połączeń z sieciami bezprzewodowymi	665
Rozdział 26. Łączenie się z siecią i korzystanie z niej	667
Używanie udostępnianych zasobów sieciowych	668
Wyświetlanie udostępnianych zasobów komputera	669
Używanie adresów sieciowych	672
Mapowanie folderu sieciowego na literę dysku lokalnego	673
Tworzenie zmapowanego folderu sieciowego	674
Mapowanie folderów za pomocą wiersza polecenia	675
Odłączanie zmapowanego folderu sieciowego	676
Tworzenie lokalizacji sieciowej dla zdalnego folderu	677
Używanie udostępnianych drukarek	679
Udostępnianie zasobów w sieci	680
Ustawianie opcji udostępniania	681
Tworzenie kont użytkowników na potrzeby udostępniania	682
Monitorowanie udostępnianych zasobów	683
Używanie plików sieciowych w trybie offline	686
Włączanie obsługi plików trybu offline	687
Udostępnianie plików lub folderów do użytku w trybie offline	688
Zmianianie ilości miejsca dla plików trybu offline	689
Blokowanie udostępniania folderu sieciowego w trybie offline	691
Szyfrowanie plików trybu offline	692
Używanie plików sieciowych w trybie offline	693
Synchronizowanie plików trybu offline	695
Radzenie sobie z konfliktami w synchronizacji	698
Rozdział 27. Zdalne połączenia sieciowe	701
Konfigurowanie zdalnego komputera jako serwera	703
Wersje systemu Windows, które mogą pełnić funkcję serwera	703
Konfigurowanie kont użytkowników na zdalnym komputerze	703

Konfigurowanie systemu Windows 7 lub Vista, aby pełnił funkcję serwera pulpitu zdalnego	704
Konfigurowanie systemu XP, aby działał jako serwer pulpitu zdalnego	707
Instalowanie pulpitu zdalnego na komputerze klienckim z systemem XP	708
Łączenie się z pulpitem zdalnym	709
Nawiązywanie podstawowego połączenia	709
Nawiązywanie zaawansowanych połączeń	711
Używanie paska połączenia	716
Odlączenie pulpitu zdalnego	716
Łączenie się z pulpitem zdalnym za pomocą internetu	717
Zmienianie portu nasłuchu	717
Konfigurowanie Zapory systemu Windows	719
Określanie adresu IP komputera zdalnego	719
Konfigurowanie przekazywania portu	720
Podłączanie pulpitu zdalnego za pomocą adresu IP i nowego portu	721
Używanie dynamicznych nazw DNS do łączenia się z siecią	721
Konfigurowanie komputera sieciowego pod kątem zdalnej administracji	722
Używanie połączeń VPN	723
Konfigurowanie bramy sieciowej na potrzeby połączenia VPN	724
Konfigurowanie klienta VPN	725
Nawiązywanie połączenia VPN	727

Rozdział 28. Przekształcanie systemu Windows 7 w serwer WWW 729

Wprowadzenie do internetowych usług informacyjnych	731
Instalowanie usług IIS	732
Wyświetlanie witryny	733
Tworzenie wyjątku Zapory systemu Windows dla serwera WWW	734
Wyświetlanie witryny z poziomu sieci	735
Wyświetlanie witryny przez internet	735
Czym jest witryna domyślna?	737
Wyświetlanie folderu domyślnej witryny	737
Wyświetlanie domyślnej witryny za pomocą menedżera usług IIS	738
Dodawanie folderów i plików do witryny domyślnej	740
Ustawianie uprawnień do folderu witryny domyślnej	740
Dodawanie plików do domyślnej witryny	741
Zmienianie strony głównej witryny domyślnej	743
Dodawanie folderu do witryny domyślnej	745
Kontrolowanie i dostosowywanie witryny	747
Zatrzymywanie witryny	747
Ponowne uruchamianie witryny	748
Zmienianie nazwy witryny domyślnej	749
Zmienianie lokalizacji witryny	749
Określanie domyślnego dokumentu witryny	750
Witryny bez dokumentu domyślnego	752
Wyłączanie dostępu anonimowego	754
Sprawdzanie dzienników serwera	756

Rozdział 29. Dodawanie komputerów Mac do sieci opartej na Windows 7	759
Sprawdzenie, czy w Mac OS X Tiger włączona jest obsługa protokołu SMB	760
Łączenie się z siecią opartą na systemie Windows	762
Łączenie się z folderami udostępnianymi w systemie Windows	763
Łączenie się z widocznym komputerem PC	764
Łączenie się z niewidocznym komputerem z systemem Windows	765
Używanie folderów udostępnianych na komputerze z systemem Windows	766
Odmontowywanie folderów udostępnianych	767
Archiwizowanie danych z Maca w folderach udostępnianych systemu Windows	767
Używanie komputerów Mac do łączenia się z pulpitem zdalnym systemu Windows 7	769
Udostępnianie udziałów z komputerów Mac systemowi Windows	772
Część VII Tworzenie skryptów w systemie Windows 7	777
Rozdział 30. Skrypty WSH w Windows 7	779
Wprowadzenie do środowiska WSH	780
Skrypty i ich wykonywanie	782
Bezpośrednie uruchamianie plików ze skryptem	783
Używanie programu WScript do uruchamiania skryptów w systemie Windows	783
Używanie programu CScript do uruchamiania skryptów z poziomu wiersza polecenia	785
Właściwości skryptów i pliki .wsh	785
Uruchamianie skryptów z uprawnieniami administratora	787
Programowanie obiektowe	789
Używanie właściwości obiektów	789
Używanie metod obiektów	790
Przypisywanie obiektu do zmiennej	792
Używanie kolekcji obiektów	792
Obiekty typu WScript	794
Wyświetlanie tekstu użytkownikom	794
Zamykanie skryptu	794
Skrypty i automatyzacja	795
Obiekty typu WshShell	800
Pobieranie obiektu typu WshShell	800
Wyświetlanie informacji użytkownikom	800
Uruchamianie aplikacji	804
Używanie skrótów	805
Zarządzanie wpisami rejestru	807
Używanie zmiennych środowiskowych	809
Obiekty typu WshNetwork	811
Pobieranie obiektu typu WshNetwork	811
Właściwości obiektu typu WshNetwork	812
Mapowanie drukarek sieciowych	812
Mapowanie dysków sieciowych	813
Przykład — obsługa Internet Explorera za pomocą skryptów	814
Wyświetlanie stron internetowych	814

Przechodzenie między stronami	815
Używanie właściwości obiektu typu InternetExplorer	815
Omówienie prostego skryptu	816
Programowanie z wykorzystaniem usługi WMI	817
Pobieranie obiektu usługi WMI	818
Pobieranie egzemplarzy klas	818
Zarządzanie zdalnymi komputerami za pomocą skryptów	822
Rozdział 31. Skrypty powłoki PowerShell	825
Wprowadzenie do powłoki PowerShell	827
Uruchamianie powłoki PowerShell	827
Wprowadzenie do cmdletów powłoki PowerShell	828
Uruchamianie cmdletów powłoki PowerShell	831
Używanie obiektów w skryptach	835
Pobieranie składowych obiektów	836
Wybieranie składowych obiektu	837
Krótkie uwagi na temat formatowania danych wyjściowych	838
Filtrowanie egzemplarzy obiektów	840
Sortowanie egzemplarzy obiektów	841
Przypisywanie obiektu do zmiennej	843
Używanie właściwości obiektów	843
Pobieranie wartości właściwości	844
Przypisywanie wartości do właściwości	844
Używanie metod obiektów	844
Używanie kolekcji obiektów	845
Tworzenie skryptów powłoki PowerShell	846
Konfigurowanie zasad wykonywania skryptów	846
Korzystanie ze zintegrowanego środowiska tworzenia skryptów powłoki PowerShell	847
Uruchamianie skryptów powłoki PowerShell	848
Część VIII Dodatki	851
Dodatek A Skróty klawiaturowe w systemie Windows 7	853
Dodatek B Krótko o protokole TCP/IP	863
Czym jest protokół TCP/IP?	865
Krótko o protokole IP	866
Budowa datagramu protokołu IP	866
Budowa adresu IP	868
Rutowanie	871
Dynamiczne przydzielanie adresów IP	874
Rozpoznawanie nazwy domeny	875
Krótko o protokole TCP	878
Gniazda TCP	878
Budowa segmentu TCP	879
Zasady pracy protokołu TCP	881
Skorowidz	883

Rozdział 19.

Zabezpieczanie sieci



W tym rozdziale:

- Zabezpieczanie sieci w Windows 7
- Ustawianie uprawnień udostępniania do folderów udostępnianych
- Ustawianie uprawnień zabezpieczeń do folderów udostępnianych
- Ukrywanie folderów udostępnianych
- Wyłączanie ukrytych współużytkowanych udziałów administracyjnych
- Usuwanie zapisanych poświadczeń pulpitu zdalnego
- Blokowanie logowania w określonych godzinach

*Nieustannie się zastanawiam,
czy ludzie naprawdę muszą poświęcać tyle energii fizycznej i umysłowej
na prowadzenie cywilizowanego życia.*

William Allingham

Kiedy połączysz ze sobą przynajmniej dwa komputery, aby zbudować sieć, zawsze pojawia się problem z bezpieczeństwem. Na poziomie użytkowników należy się upewnić, że inne osoby mają dostęp tylko do tych części systemu, które uznałeś za odpowiednie do użytku publicznego. Nikt — nawet znajomi i administratorzy — nie powinien mieć możliwości zaglądania do prywatnych obszarów komputera. Na poziomie sieci administratorzy muszą się upewnić, że komputery mają odpowiednie ograniczenia dostępu.

Jeśli chcesz kontrolować nie tylko to, kto ma dostęp do danych, ale też to, co użytkownicy z nimi robią, musisz zastosować kilka środków ostrożności z zakresu bezpieczeństwa sieci. Oczywiście, jednym z problemów jest to, że inni użytkownicy zobaczą dane, których nie powinni wykorzystywać. Kolejny kłopot to niewiarygodny dostęp intruzów do sieci. Na szczęście możesz zminimalizować prawdopodobieństwo takich ataków. W tym rozdziale poznasz szereg przydatnych technik zabezpieczania sieci.

Pamiętaj, że bezpieczeństwo sieci zależy też od zabezpieczeń komputerów klienckich, dlatego koniecznie zapoznaj się ze wskazówkami i technikami, które pomogą Ci zabezpieczyć system Windows 7 w większym stopniu niż rozwiązania opisane w poprzednich rozdziałach. Ponadto z rozdziału 20., „Zwiększanie bezpieczeństwa sieci bezprzewodowej”, dowiesz się, jak zabezpieczyć sieć bezprzewodową.

Zabezpieczanie sieci w Windows 7

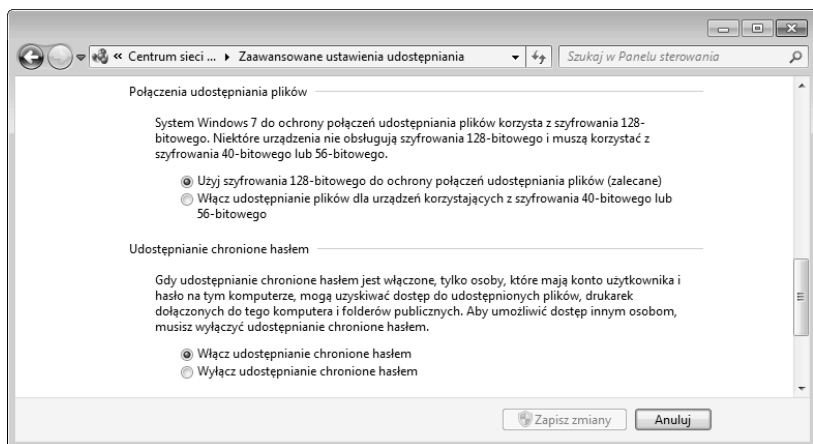
Zabezpieczenia sieci w Windows 7 są domyślnie ustawione na wysokim poziomie, jednak trzeba zrobić kilka rzeczy, aby zmaksymalizować bezpieczeństwo środowiska sieciowego. Upewnij się, że włączone jest udostępnianie chronione hasłem. Wyłącz niskopoziomowy kreator udostępniania, aby zamiast niego można było wykorzystać wysokopoziomowe uprawnienia.

Upewnianie się, że włączone jest udostępnianie chronione hasłem

Udostępnianie chronione hasłem polega na tym, że osoby, które mają dostęp do udziałów sieciowych, muszą znać nazwę użytkownika i hasło konta z danego systemu. Jest to najbezpieczniejszy sposób na współużytkowanie udziałów sieciowych, dlatego w Windows 7 ochrona hasłem jest domyślnie włączona. Jeżeli bezpieczeństwo sieci ma dla Ciebie jakiegokolwiek znaczenie (w przeciwnym razie zastanawiam się, dlaczego czytasz ten rozdział), warto poświęcić chwilę na upewnienie się, że omawiana funkcja jest włączona:

1. Kliknij ikonę *Sieć* w obszarze powiadomień.
2. Kliknij łącze *Otwórz Centrum sieci i udostępniania*.
3. W nowym oknie kliknij łącze *Zmień zaawansowane ustawienia udostępniania*. Windows 7 otworzy okno *Zaawansowane ustawienia udostępniania*.
4. W obszarze *Dom i praca* znajdź kategorię *Udostępnianie chronione hasłem* i wybierz opcję *Włącz udostępnianie chronione hasłem*, jak ilustruje to rysunek 19.1.

Rysunek 19.1.
Zaznacz opcję *Włącz udostępnianie chronione hasłem*



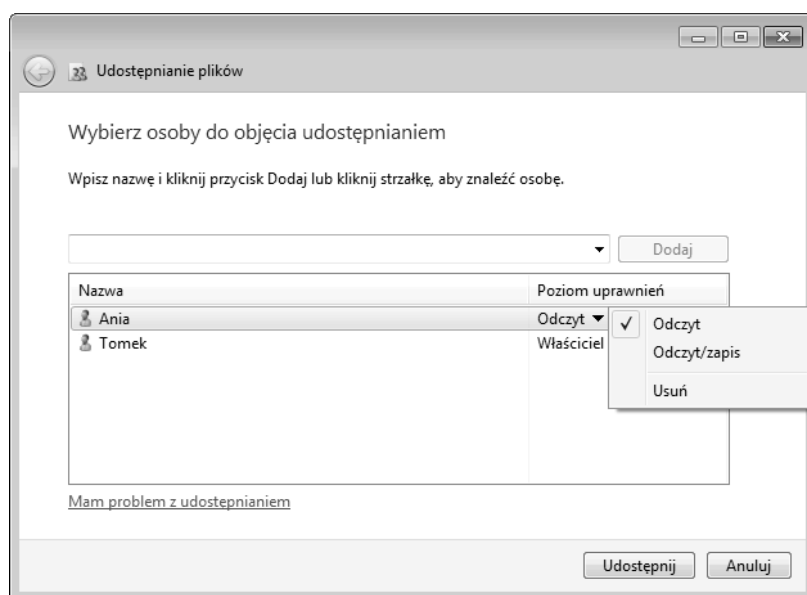
5. Kliknij przycisk *Zapisz zmiany*.

Wyłączanie kreatora udostępniania

Udostępnianie bywa skomplikowane, kiedy wymaga zarządzania uprawnieniami i innymi szczegółami. Ta książka poświęcona jest właśnie detalom systemu Windows 7, dlatego udostępnianie nie powinno przerażać takich użytkowników, jak Ty lub ja. Jednak nowicjusze zwykle chcą, aby proces ten był łatwy i prosty. Dla takich osób w Windows 7 wbudowano kreator udostępniania. Ten mechanizm oferuje ostrożnym użytkownikom ograniczony zestaw opcji i metod informowania innych osób o obecności udostępnianych udziałów.

Kreator udostępniania jest domyślnie włączony. Wkrótce dowiesz się, jak to zmienić. Aby wiedzieć, z czego rezygnujesz, popatrz na początkowe okno dialogowe, widoczne na rysunku 19.2. Aby je otworzyć, kliknij folder lub plik prawym przyciskiem myszy i wybierz opcję *Udostępnij/Określonym osobom*. Określ za pomocą listy konta użytkowników komputera, a następnie przypisz wybranym osobom jeden z dwóch poziomów uprawnień — *Odczyt* (tylko do odczytu) lub *Odczyt/zapis* (do odczytu i zapisu). Kiedy klikniesz przycisk *Udostępnij*, kreator udostępniania wyświetli adres zasobu i prowadzący do niego odnośnik, który można przesłać e-mailem do innych użytkowników.

Rysunek 19.2.
Kreator udostępniania to prosty, przeznaczony dla nowicjuszy interfejs do udostępniania udziałów



Kreator udostępniania to odpowiednie rozwiązanie dla początkujących. Jednak pozostali użytkownicy chcą zwykle korzystać z pełni możliwości związanych z uprawnieniami i innymi ciekawymi technikami. Aby uzyskać do nich dostęp, należy wyłączyć kreator udostępniania. W tym celu wykonaj poniższe operacje:

1. Otwórz menu *Start*, wpisz słowo **folder**, a następnie kliknij nazwę *Opcje folderów* w wynikach wyszukiwania (możesz też w dowolnym oknie folderów wybrać opcję *Organizuj/Opcje folderów i wyszukiwania*).
2. Wyświetl zakładkę *Widok*.
3. Usuń zaznaczenie pola *Użyj Kreatora udostępniania*.
4. Kliknij przycisk *OK*.

Ustawianie uprawnień udostępniania do folderów udostępnianych

Kiedy kreator udostępniania plików jest wyłączony, możesz przy udostępnianiu folderów użyć zaawansowanych uprawnień. Pozwalają one określić, kto ma dostęp do folderów i co dani użytkownicy mogą z nimi robić. Możesz też ustawić zaawansowane uprawnienia dla całych grup zamiast dla poszczególnych kont. Jeśli na przykład przyznasz uprawnienia grupie administratorów, zostaną one automatycznie powiązane ze wszystkimi jej członkami.

- Zanim przejdiesz dalej, upewnij się, że przygotowałeś konto dla każdej osoby, która ma mieć dostęp do zasobu (zobacz punkt „Tworzenie kont użytkowników i zarządzanie nimi” na stronie 470).

Wykonaj poniższe operacje, aby udostępnić folder z zastosowaniem zaawansowanych uprawnień:

1. W Eksploratorze systemu Windows zaznacz folder, który chcesz udostępnić. Jeśli planujesz udostępnić podfolder lub plik, otwórz katalog, w którym znajduje się dany obiekt. Następnie kliknij właściwy podfolder lub plik.
2. Kliknij przycisk *Udostępnij* w okienku zadań, a następnie wybierz opcję *Udostępnianie zaawansowane*. Windows 7 wyświetli ekran właściwości obiektu z otwartą zakładką *Udostępnianie*.

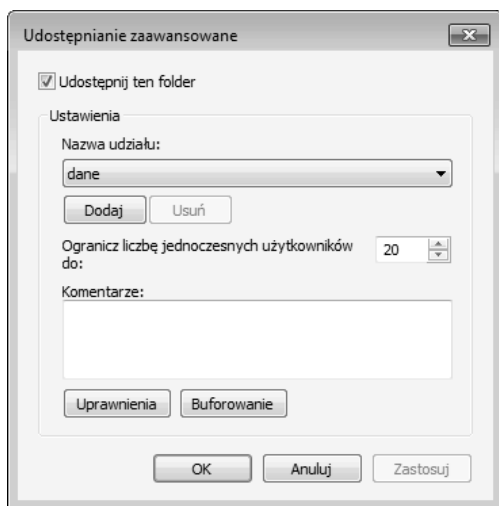
Wskazówka



Możesz też kliknąć folder prawym przyciskiem myszy i wybrać opcję *Udostępnij/Udostępnianie zaawansowane*.

3. Kliknij przycisk *Udostępnianie zaawansowane*. Pojawi się okno dialogowe o tej samej nazwie.
4. Zaznacz pole *Udostępnij ten folder*, co przedstawia rysunek 19.3.
5. Domyślnie Windows 7 wykorzystuje nazwę folderu jako nazwę udostępnianego udziału. Jeśli wolisz inne określenie, wprowadź zmiany w polu *Nazwa udziału*.
6. W małych sieciach zwykle nie trzeba ograniczać liczby osób, które mają dostęp do danego zasobu, dlatego możesz pozostawić w polu *Ogranicz liczbę jednoczesnych użytkowników do* wartość 20.
7. Kliknij przycisk *Uprawnienia*, aby wyświetlić okno dialogowe *Uprawnienia dla „dane”*, gdzie „dane” to nazwa udziału określona w kroku 5.
8. Wybierz grupę *Wszyscy* na liście *Nazwy grup lub użytkowników*, a następnie kliknij przycisk *Usuń*.
9. Kliknij przycisk *Dodaj*, aby wyświetlić okno dialogowe *Wybieranie: Użytkownicy lub Grupy*.

Rysunek 19.3.
Zaznacz pole
Udostępnij ten folder



Uwaga



Jak wskazuje nazwa, grupa **Wszyscy** obejmuje każdego użytkownika. Zawsze najlepiej jest usunąć tę grupę, aby móc przypisać uprawnienia do określonych grup lub kont.

10. W polu tekstowym *Wprowadź nazwy obiektów do wybrania* wpisz nazwy użytkowników, którym chcesz przyznać uprawnienia do udostępnianego udziału (poszczególne nazwy rozdziel średnikami). Kiedy to zrobisz, kliknij przycisk **OK**.

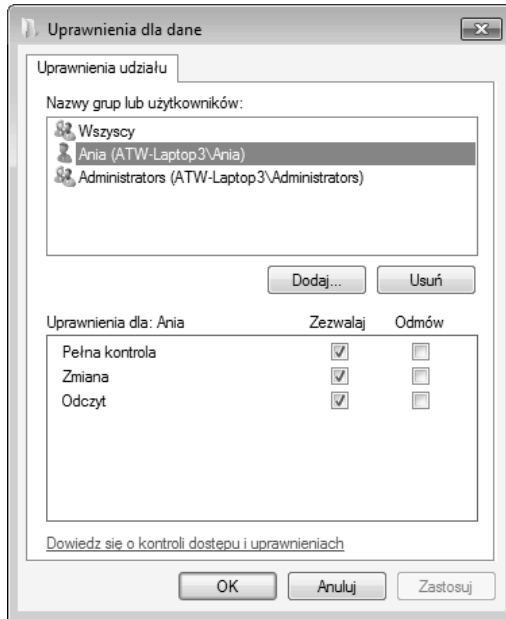
Wskazówka



Jeśli nie jesteś pewny, jak zapisać nazwę użytkownika lub grupy, kliknij przycisk *Zaawansowane*, aby wyświetlić zaawansowaną wersję okna dialogowego *Wybieranie: Użytkownicy lub Grupy*, a następnie kliknij przycisk *Znajdź teraz*. Windows 7 wyświetli listę wszystkich dostępnych użytkowników i grup. Zaznacz nazwę, którą chcesz wykorzystać, a następnie kliknij przycisk **OK**.

11. Zaznacz użytkownika na liście *Nazwy grup lub użytkowników*.
12. Za pośrednictwem listy *Uprawnienia* (zobacz rysunek 19.4) możesz włączyć lub wyłączyć następujące uprawnienia:
 - **Odczyt.** Umożliwia grupie lub użytkownikowi jedynie odczyt zawartości folderu lub pliku. Dana osoba nie ma uprawnień do wprowadzania jakichkolwiek zmian w tych obiektach.

Rysunek 19.4.
Użyj okna dialogowego
Uprawnienia w celu
określenia uprawnień
do udostępnianego
udziału



- **Zmiana.** Powoduje nadanie grupie lub użytkownikowi uprawnienia *Odczyt* i umożliwia modyfikowanie zawartości udostępnianego udziału.
 - **Pełna kontrola.** Powoduje nadanie grupie lub użytkownikowi uprawnienia *Zmiana* i umożliwia przejęcie udostępnianego udziału na własność.
13. Powtórz kroki od 9. do 12., aby dodać i skonfigurować inne konta lub grupy.
 14. Kliknij przycisk *OK*, aby wrócić do okna dialogowego *Udostępnianie zaawansowane*.
 15. Kliknij przycisk *OK*, aby wrócić do zakładki *Udostępnianie*.
 16. Kliknij przycisk *Zamknij*, aby udostępnić udział w sieci.

Ustawienia uprawnień zabezpieczeń do folderów udostępnianych

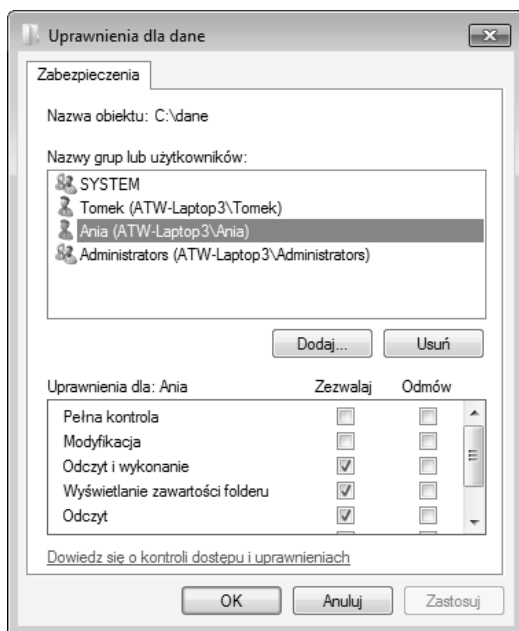
Jeśli chcesz uzyskać jeszcze większą kontrolę nad udziałami udostępnianymi w sieci, powinieneś dodatkowo ustawić uprawnienia zabezpieczeń systemu NTFS. Przypominają one uprawnienia udostępniania, jednak umożliwiają zmianę większej liczby opcji.

Proces ustawiania uprawnień zabezpieczeń do udostępnianych folderów wygląda tak:

1. W Eksploratorze Windows kliknij prawym przyciskiem myszy folder, którego chcesz użyć, a następnie wybierz opcję *Właściwości*, aby wyświetlić okno dialogowe o tej samej nazwie.

2. Otwórz zakładkę *Zabezpieczenia*.
3. Kliknij przycisk *Edytuj*, aby otworzyć okno dialogowe *Uprawnienia dla „folder”*, gdzie „folder” to nazwa katalogu. Jak widać na rysunku 19.5, okno to przypomina ekran do ustawiania uprawnień udostępniania, który przedstawiono wcześniej (zobacz rysunek 19.4).

Rysunek 19.5.
Użyj tej wersji okna dialogowego *Uprawnienia*, aby określić uprawnienia zabezpieczeń do udostępnianego udziału



4. Aby zastosować istniejące uprawnienia, zaznacz grupę lub użytkownika i przejdź do kroku 10.
5. Jeśli chcesz dodać nowe uprawnienia, kliknij przycisk *Dodaj*, aby wyświetlić okno dialogowe *Wybieranie: Użytkownicy lub Grupy*.
6. W polu tekstowym *Wprowadź nazwy obiektów do wybrania* wpisz nazwy użytkowników, którym chcesz przyznać uprawnienia do udostępnianego udziału (poszczególne nazwy rozdziel średnikami).
7. Kliknij przycisk *OK*, aby wrócić do okna *Uprawnienia*.
8. Zaznacz użytkownika na liście *Nazwy grup lub użytkowników*.
9. Użyj pól wyboru *Zezwalaj* i *Odmów* na liście *Uprawnienia*, aby włączyć lub wyłączyć poszczególne uprawnienia.
 - Zobacz punkt „Przypisywanie standardowych uprawnień” na stronie 446.
10. Powtórz kroki od 5. do 9., aby dodać i skonfigurować inne konta lub grupy.
11. Kliknij przycisk *OK*, aby wrócić do zakładki *Zabezpieczenia*.
12. Kliknij przycisk *OK*, aby zastosować nowe ustawienia zabezpieczeń.

Ukrywanie folderów udostępnianych

Dodanie silnych haseł do kont, a następnie przyznanie użytkownikom uprawnień do udostępnianych folderów to niezbędne operacje zabezpieczające sieć. W większości małych sieci wystarczy to do zapewnienia odpowiedniego poziomu bezpieczeństwa. Jednak kiedy chronisz sieć, następnym skutecznym „narzędziem” jest „paranoiczne nastawienie”. Na przykład odpowiednio podejrzliwy administrator sieci nie zakłada, że nikt nie zdoła się do niej włamać. Wprost przeciwnie — przyjmuje, że któregoś dnia ktoś *uzyska* dostęp, dlatego zastanawia się, co zrobić, aby zminimalizować potencjalne szkody.

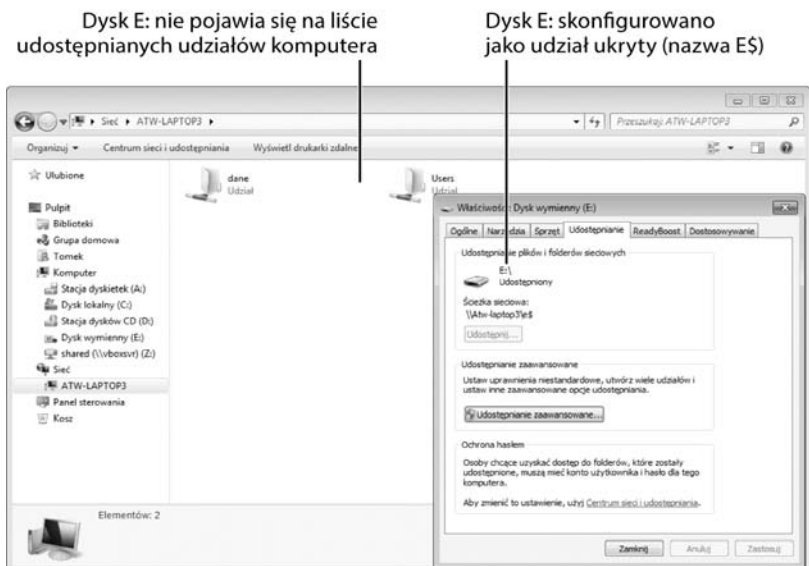
Jedną z pierwszych rzeczy, jaką robią (lub powinni robić) „paranoiczni” administratorzy, jest ukrycie cennych, prywatnych lub wrażliwych danych. Jeśli na przykład udostępniasz folder o nazwie *Poufne dokumenty*, zachęcasz potencjalnego złodzieja, aby zajrzał do tego katalogu. To prawda, możesz zmienić nazwę na mniej prowokującą, ale napastnik może dotrzeć do takiego folderu choćby przypadkiem. Aby temu zapobiec, możesz udostępnić udział i jednocześnie ukryć go.

Ukrywanie udostępnianych folderów jest bardzo proste. Kiedy tworzysz udział, dodaj symbol dolara (\$) na końcu nazwy. Jeśli na przykład udostępniasz dysk L:, nazwij go L\$. Zapobiega to wyświetlaniu udziału na liście zasobów, kiedy wyświetlasz zawartość zdalnego komputera w oknie *Sieć*.

Aby zobaczyć, jak działa ta technika, przyjrzyj się rysunkowi 19.6. W oknie dialogowym *Właściwości* dysku E: zobaczysz, że udział jest udostępniany za pomocą następującej ścieżki:

```
\\ATW-laptop3\e$.
```

Rysunek 19.6. Ukryte udostępniane udziały (takie jak widoczny tu dysk E:) nie pojawiają się na liście współużytkowanych zasobów komputera



Oznacza to, że udział jest udostępniany pod nazwą *E:* na komputerze ATW-LAPTOP3. Jednak w oknie folderów dysk *E:* nie jest widoczny na liście zasobów udostępnianych przez tę maszynę.

Ostrzeżenie



Ukrywanie udziałów pozwala powstrzymać przeciętnych użytkowników, jednak doświadczony włamywacz prawdopodobnie zna sztuczkę z symbolem \$. Dlatego powinieneś nadać ukrytym zasobom nieoczywiste nazwy.

Jak uzyskać dostęp do ukrytego zasobu? Musisz oczywiście znać jego nazwę, co pozwoli Ci zastosować poniższe techniki:

- Użyj kombinacji klawiszów *Windows+R* (lub wybierz opcję *Start/Wszystkie programy/Akcesoria/ Uruchom*), aby otworzyć okno dialogowe *Uruchom*. Wpisz nazwę ukrytego udziału i kliknij przycisk *OK*. Aby na przykład wyświetlić ukryty zasób *E\$* z komputera ATW-LAPTOP3, wpisz polecenie:
\\atw-laptop3\e\$.
- W wierszu polecenia wpisz instrukcję **start**, odstęp i ścieżkę sieciową, a następnie wciśnij klawisz *Enter*. Aby uzyskać dostęp do ukrytego udziału *E\$* z komputera ATW-LAPTOP3, wpisz polecenie:
start \\atw-laptop3\e\$.
- Użyj opcji *Mapuj dysk sieciowy*, którą opisuję w rozdziale 26., „Łączenie się z siecią i korzystanie z niej”. W polu tekstowym *Folder*, w oknie dialogowym *Mapowanie dysku sieciowego*, wpisz ścieżkę UNC do ukrytego udziału.
- Szczegółowe informacje o mapowaniu udostępnianych folderów znajdziesz w punkcie „Mapowanie folderu sieciowego na literę dysku lokalnego” na stronie 673.
- Aby uzyskać dostęp do ukrytych drukarek, zastosuj się do instrukcji łączenia się ze współużytkowanymi drukarkami; instrukcje te przedstawiam w rozdziale 26. Kiedy Windows 7 zacznie szukać dostępnych urządzeń, wybierz opcję *Szukanej drukarki nie ma na liście* i kliknij przycisk *Dalej*. W oknie dialogowym, które się pojawi, podaj w polu tekstowym *Drukarka* ścieżkę sieciową do ukrytej drukarki.
- Więcej informacji o używaniu drukarek sieciowych znajdziesz w punkcie „Używanie udostępnianych drukarek” na stronie 679.

Wyłączanie ukrytych współużytkowanych udziałów administracyjnych

W poprzednim podrozdziale wspomniałem, że możesz dodać do nazwy symbol \$, aby ukryć dany udział. Warto też zmienić nazwę zasobu w taki sposób, aby szpiegdy nie mogli łatwo odgadnąć zawartości folderu. Ponadto Windows 7 tworzy dla celów administracyjnych określone ukryte udziały, między innymi dla dysku C: (C\$) i innych partycji dysku twardego obecnych w systemie. System dodaje następujące obiekty:

Udział	Ścieżka do udostępnianego udziału	Przeznaczenie
ADMIN\$	%SystemRoot%	Zdalna administracja
IPC\$	Brak	Zdalna komunikacja między procesami

Aby wyświetlić te zasoby, wybierz *Start/Wszystkie programy/Akcesoria/Wiersz polecenia*, aby uruchomić wiersz polecenia. Wpisz instrukcję **net share** i wciśnij klawisz *Enter*. Zobaczysz listę podobną do poniższej:

Udział	Zasób	Uwaga
C\$	C:\	Domyślny udział
D\$	D:\	Domyślny udział
ADMIN	C:\Windows	Administracja zdalna
IPC\$		Zdalne wywołanie IPC

Choć C\$, D\$ i ADMIN\$ to udziały ukryte, są jednocześnie dobrze znane. Powoduje to niewielkie zagrożenie w obszarze bezpieczeństwa, związane z możliwością uzyskania dostępu do sieci przez intruza.

Aby zlikwidować tę lukę, możesz wymusić na systemie Windows 7 wyłączenie tych udziałów. Należy to zrobić w następujący sposób:

1. Otwórz menu *Start*, wpisz instrukcję **regedit**, a następnie wciśnij klawisz *Enter*. Pojawi się okno dialogowe kontroli konta użytkownika.
2. Wprowadź poświadczenia, aby kontynuować. Windows 7 otworzy edytor rejestru.

Ostrzeżenie



Pamiętaj, że rejestr zawiera wiele ważnych ustawień, które są niezbędne do właściwego funkcjonowania systemu Windows 7 i różnych programów. Dlatego, kiedy używasz edytora rejestru, nie wprowadzaj innych zmian niż opisane w książce.

3. Otwórz węzeł *HKEY_LOCAL_MACHINE*.
4. Otwórz węzeł *SYSTEM*.
5. Otwórz węzeł *CurrentControlSet*.
6. Otwórz węzeł *Services*.
7. Otwórz węzeł *LanmanServer*.
8. Zaznacz węzeł *Parameters*.
9. Wybierz opcję *Edycja/Nowy/Wartość DWORD (32-bitowa)*. Windows 7 doda nową wartość do klucza *Parameters*.
10. Wpisz ustawienie **AutoShareWks** i wciśnij klawisz *Enter*. Możesz zostawić dla nowego ustawienia wartość domyślną (0).
11. Ponownie uruchom Windows 7, aby zastosować nowe ustawienia.

Po raz kolejny wybierz opcję *Start/Wszystkie programy/Akcesoria/Wiersz polecenia*, aby otworzyć wiersz polecenia. Wpisz instrukcję **net share** i wciśnij klawisz *Enter*. Tym razem zobaczysz następujące dane:

Udział	Zasób	Uwaga
IPC\$		Zdalne wywołanie IPC

Ostrzeżenie

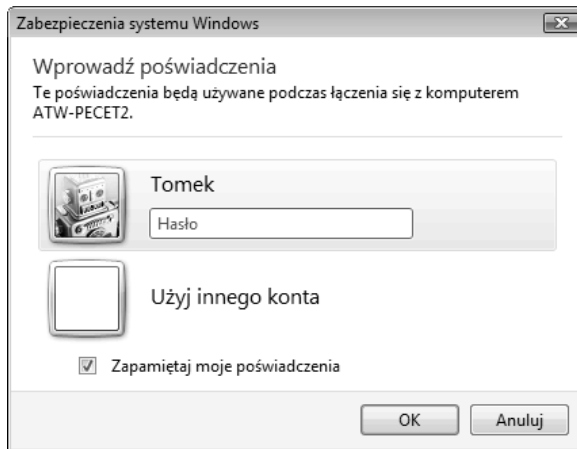


Niektóre programy oczekują, że udziały administracyjne będą dostępne, dlatego ich wyłączenie może spowodować, iż takie aplikacje przestaną działać lub wygenerują komunikat o błędzie. Jeśli tak się stanie, włącz odpowiednie udziały. W tym celu otwórz edytor rejestru i albo usuń ustawienie *AutoShareWks*, albo zmień jego wartość na 1.

Usuwanie zapisanych poświadczeń pulpitu zdalnego

Kiedy logujesz się do komputera w sieci za pomocą funkcji *Podłączanie pulpitu zdalnego* (zobacz rozdział 27., „Zdalne połączenia sieciowe”), w oknie dialogowym logowania znajduje się pole o nazwie *Zapamiętaj moje poświadczenia*, co ilustruje rysunek 19.7. Jeśli zaznaczysz to pole, Windows 7 nie zażąda hasła, kiedy w przyszłości spróbujesz połączyć się z danym komputerem.

Rysunek 19.7.
Funkcja Podłącz pulpit zdalny umożliwia zapisanie danych uwierzytelniających używanych do logowania



- Aby dowiedzieć się, jak zalogować się za pomocą funkcji Podłączanie pulpitu zdalnego, zobacz punkt „Łączenie się z pulpitem zdalnym” na stronie 709.

Jest to z pewnością wygodne, jednak powoduje lukę w zabezpieczeniach, ponieważ oznacza, że każdy, kto ma dostęp do danej maszyny, będzie mógł też wykorzystać pulpit zdalny komputera. Dlatego nigdy nie należy zaznaczać pola *Zapamiętaj moje poświadczenia*.

Co jednak zrobić, jeśli omawiana opcja była wcześniej zaznaczona? Na szczęście można rozwiązać ten problem, ponieważ Windows 7 pozwala usunąć zapisane dane uwierzytelniające.

Ostrzeżenie

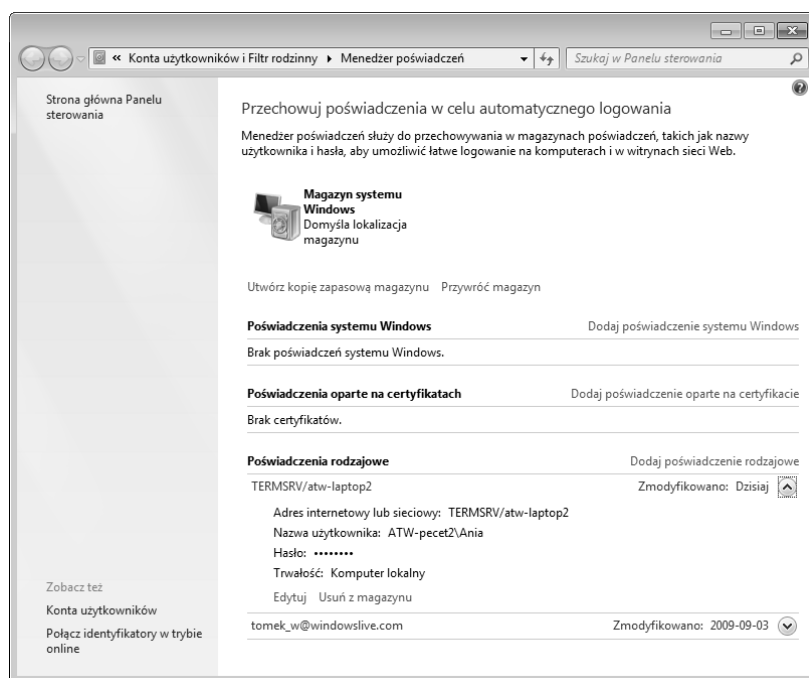


W zakładce *Ogólne*, w oknie dialogowym *Podłączanie pulpitu zdalnego* (wybierz *Start/Wszystkie programy/Akcesoria/Podłączanie pulpitu zdalnego*), znajduje się pole wyboru o nazwie *Zawsze pytaj o poświadczenia* (możliwe, że będziesz musiał kliknąć przycisk *Opcje*, aby je wyświetlić). Na pozór zaznaczenie tego pola pozwala zabezpieczyć połączenie. Jednak Windows 7 nadal zapisuje dane uwierzytelniające i żeby ich użyć, wystarczy usunąć zaznaczenie pola *Zawsze pytaj o poświadczenia*.

Oto operacje, które powinieneś wykonać:

1. Otwórz menu *Start*, wpisz słowo **poświadczenia**, a następnie wciśnij klawisz *Enter*. Windows 7 wyświetli okno *Menedżer poświadczeń*.
2. Kliknij poświadczenia, które chcesz usunąć. Nazwy poświadczeń funkcji Podłączanie pulpitu zdalnego zawsze zaczynają się od sekwencji „TERMSRV” (to skrót od ang. *Terminal Server*). Menedżer wyświetli szczegółowe informacje o poświadczeniach, co ilustruje rysunek 19.8.

Rysunek 19.8.
Możesz użyć Menedżera poświadczeń do usunięcia zapisanych poświadczeń logowania z funkcji Podłączenie pulpitu zdalnego



3. Kliknij przycisk *Usuń z magazynu*. Menedżer poświadczeń wyświetli komunikat z prośbą o zatwierdzenie operacji.
4. Kliknij przycisk *Tak*.
5. Powtórz kroki od 2. do 4., aby usunąć inne zapisane poświadczenia funkcji Podłączenie pulpitu zdalnego.

Wskazówka



Inny sposób na usunięcie zapisanych poświadczeń pulpitu zdalnego wymaga wybrania *Start/Wszystkie programy/Akcesoria/Podłączenie pulpitu zdalnego*. W oknie dialogowym *Podłączenie pulpitu zdalnego* kliknij przycisk *Opcje*, aby rozwinąć to okno; otwórz zakładkę *Ogólne*, a następnie kliknij łącze *usunąć* w obszarze *Ustawienia logowania*. Kliknij przycisk *Tak*, kiedy zobaczysz monit o zatwierdzenie operacji.

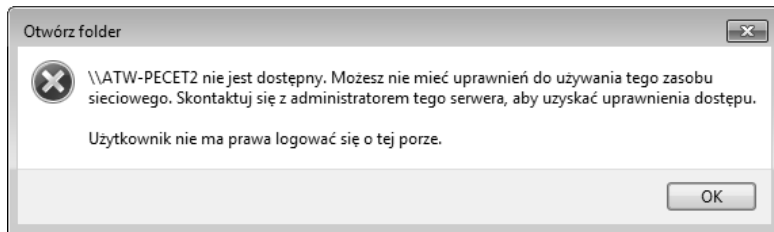
Blokowanie logowania w określonych godzinach

Jeśli skonfigurowałeś konta w taki sposób, aby inni użytkownicy sieci mogli korzystać z Twojego komputera, domyślnie osoby te będą mogły przeglądać udziały i używać ich o dowolnej porze. Zwykle nie stanowi to problemu, jednak możesz też zablokować dostęp do systemu w określonych godzinach. Jeśli na przykład każdego popołudnia używasz do pracy pewnego udostępnianego folderu, możesz nie chcieć, aby w tym czasie korzystały z niego inne osoby.

Windows 7 umożliwia wskazanie dni tygodnia i godzin dnia, w których określony użytkownik może logować się do systemu. Jeśli dana osoba spróbuje uzyskać dostęp do komputera w innym czasie, zobaczy okno podobne do widocznego na rysunku 19.9.

Rysunek 19.9.

Jeśli określisz godziny logowania dla użytkownika, osoba ta zobaczy okno dialogowe podobne do powyższego, kiedy spróbuje zalogować się w innym czasie



W kilku następnych punktach opisuję korzystanie z tej funkcji.

Określanie godzin logowania użytkownika

Niestety, Windows 7 nie udostępnia okna dialogowego ani innego interfejsu do ustawiania godzin logowania użytkownika. Musisz skorzystać z wiersza polecenia i wpisać w nim instrukcję o poniższej, ogólnej składni:

```
net user nazwa_użytkownika /times:dzień1,godziny1;dzień2,godziny2,...
```

nazwa_użytkownika Nazwa konta, które chcesz ustawić.

dzień1, dzień2 Dzień tygodnia, w którym użytkownik może się logować. Możesz podać całe nazwy dni, jednak szybsze jest wpisywanie ich kodów (wielkość znaków nie ma znaczenia): Su, M, T, W, Th, F i Sa. Można też określić przedział, na przykład M-F (od poniedziałku do piątku).

godziny1, godziny2 Zakres godzin, w których użytkownik może się logować w danym dniu. Składnia określania przedziału to *początek-koniec*, gdzie *początek* określa początek godzin logowania, a *koniec* — ich koniec. Obsługiwany jest zapis 24- i 12-godzinny, jednak w tym drugim przypadku trzeba dodać przyrostek AM lub PM.

Oto kilka przykładów:

```
net user kasia /times:M-F,9AM-5PM
net user stefan /times:M,18-24
net user emilka /times:Sa,10PM-6PM; Su,12PM-6PM
```

Wskazówka



Po ustawieniu godzin logowania użytkownika w przyszłości możesz zechcieć usunąć ograniczenia. Aby przyznać danej osobie dostęp we wszystkich godzinach, zastosuj parametr **all**:

```
net user kasia /times:all
```

Aby w ogóle pozbawić użytkownika dostępu, nie podawaj żadnych parametrów:

```
net user jacek /times:
```

Wykonaj poniższe operacje, aby określić godziny logowania użytkownika:

1. Otwórz menu *Start* i wpisz słowo **wiersz**.
2. W wynikach wyszukiwania kliknij prawym przyciskiem myszy nazwę *Wiersz polecenia* i wybierz opcję *Uruchom jako administrator*. Pojawi się okno kontroli konta użytkownika.
3. Wpisz poświadczenia KKU, aby kontynuować. Windows 7 otworzy wiersz polecenia z uprawnieniami administratora.
4. Wpisz odpowiednią instrukcję **net user /times** i wciśnij klawisz *Enter*. Instrukcja **NET USER** wyświetli komunikat *Polecenie zostało wykonane pomyślnie*.
5. Powtórz krok 4., aby wprowadzić wszystkie potrzebne godziny logowania.
6. Wpisz instrukcję **exit** i wciśnij klawisz *Enter*, aby zamknąć wiersz polecenia.

Automatyczne wylogowywanie użytkownika po upłynięciu godzin logowania

Domyślnie Windows 7 nie robi nic, jeśli godziny logowania upłyną w momencie, kiedy użytkownik korzysta z komputera. Oznacza to, że nie możesz powstrzymać nastolatka przed surfowaniem po internecie przez całą noc. Aby rozwiązać ten problem, możesz skonfigurować Windows 7 tak, aby automatycznie wylogowywał użytkownika, kiedy upłyną godziny logowania. Oto, jak to zrobić:

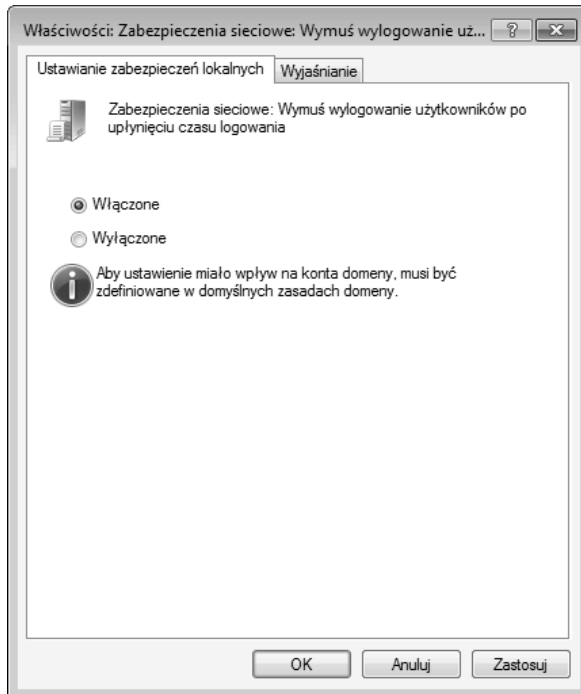
Uwaga



Opisane operacje wymagają dostępu do przystawki *Zasady zabezpieczeń lokalnych*, która jest dostępna tylko w wersjach **Professional**, **Enterprise** i **Ultimate** systemu Windows 7.

1. Otwórz menu *Start*, wpisz nazwę **secpol.msc** i wciśnij klawisz *Enter*.
2. Otwórz węzeł *Ustawienia zabezpieczeń/Zasady lokalne/Opcje zabezpieczeń*.
3. Kliknij dwukrotnie zasadę *Zabezpieczenia sieciowe: Wymuś wylogowanie użytkowników po upływie czasu logowania*.
4. Wybierz opcję *Włączone*, jak przedstawia to rysunek 19.10.

Rysunek 19.10.
Włącz zasadę
Zabezpieczenia
sieciowe: Wymuś
wylogowanie
użytkowników
po upływie czasu
logowania



5. Kliknij przycisk *OK*.