

## » 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. Zaawansowana administracja systemem

Autor: Andrzej Szelaąg  
ISBN: 978-83-246-2461-4  
Format: 158x235, stron: 360



Komfortową metodę wprowadzenia w zaawansowane zagadnienia związane z zarządzaniem nowym środowiskiem firmy Microsoft oferuje książka Windows 7 PL. Zaawansowana administracja systemem. Dzięki niej poznasz m.in. dostępne wersje systemu Windows 7 PL oraz dowiesz się, jakie wprowadzono w nich nowości, a także wybierzesz najlepszy sposób instalacji tego środowiska. Poza tym nauczysz się korzystać z narzędzi administracyjnych, systemowych i narzędziowych oraz zdobędziesz wiadomości na temat zaawansowanego zarządzania dyskami i systemami plików w Windows 7 PL. Łatwo opanujesz też administrację kontami użytkowników i grup oraz poznasz tematykę bezpieczeństwa środowiska i zagadnienia związane z korzystaniem z sieci.

- Wprowadzenie do systemu Windows 7 PL
- Wybór wersji i instalacja środowiska
- Zarządzanie komputerem z systemem Windows 7 PL
- Administracja dyskami i systemami plików
- Zarządzanie kontami użytkowników i grupami
- Zaawansowana konfiguracja i używanie narzędzi do ochrony danych
- Zarządzanie ustawieniami sieci i dostępem do internetu
- Konfiguracja zabezpieczeń systemu
- Monitorowanie i optymalizacja działania Windows 7 PL

**Już dziś zostań profesjonalnym administratorem systemu Windows 7 PL**

# Spis treści

<b>Wstęp .....</b>	<b>9</b>
<b>Rozdział 1. Wprowadzenie do systemu Windows 7 .....</b>	<b>15</b>
1.1. Rodzina systemów Windows 7 .....	15
1.1.1. Windows 7 Starter .....	16
1.1.2. Windows 7 Home Basic .....	16
1.1.3. Windows 7 Home Premium .....	16
1.1.4. Windows 7 Professional .....	17
1.1.5. Windows 7 Ultimate .....	18
1.1.6. Windows 7 Enterprise .....	20
1.2. Dlaczego warto wybrać system Windows 7? .....	21
1.2.1. Łatwość, prostota i intuicyjność użytkowania systemu .....	21
1.2.2. Uprozczone zarządzanie sprzętem i aplikacjami .....	28
1.2.3. Rozszerzone możliwości zarządzania danymi .....	34
1.2.4. Zwiększona wydajność i skalowalność .....	35
1.2.5. Ulepszony system zabezpieczeń i ochrony danych .....	36
<b>Rozdział 2. Zaawansowana instalacja systemu Windows 7 .....</b>	<b>43</b>
2.1. Przygotowanie do instalacji .....	43
2.1.1. Architektura 32 czy 64 bity? .....	44
2.1.2. Uaktualnienie systemu czy czysta instalacja? .....	44
2.1.3. Jaki układ partycji dyskowych i system plików? .....	45
2.1.4. Partycjonowanie MBR czy GPT? .....	47
2.1.5. Sprawdzenie minimalnych wymagań sprzętowych .....	48
2.1.6. Konfigurowanie ustawień BIOS .....	48
2.2. Instalacja systemu Windows 7 Professional .....	49
2.2.1. Wymagania specjalne dla dysków podstawowych i dynamicznych .....	49
2.2.2. Instalowanie systemu Windows 7 Professional za pomocą skryptu DiskPart.exe .....	50
2.3. Czynności poinstalacyjne .....	55
2.3.1. Personalizowanie systemu .....	55
2.3.2. Uaktualnienie systemu .....	58
2.3.3. Pobieranie i instalowanie programu antywirusowego .....	63
<b>Rozdział 3. Zarządzanie komputerem z systemem Windows 7 .....</b>	<b>65</b>
3.1. Przystawka Zarządzanie komputerem (CompMgmt.msc) .....	65
3.1.1. Korzystanie z narzędzi systemowych .....	67
3.1.2. Korzystanie z narzędzia Magazyn .....	80
3.1.3. Zarządzanie usługami systemowymi i aplikacjami .....	81

3.2. Wybrane narzędzia administracyjne i systemowe .....	82
3.2.1. Zasady zabezpieczeń lokalnych (SecPol.msc) .....	82
3.2.2. Konfiguracja systemu (MSConfig.exe) .....	83
3.2.3. Informacje o systemie (MSInfo32.exe) .....	85
3.2.4. Windows Management Interface Command-line (WMIC.exe) .....	85
3.3. Panel sterowania (Control.exe) .....	92
3.3.1. System i zabezpieczenia .....	93
3.3.2. Sieć i Internet .....	95
3.3.3. Sprzęt i dźwięk .....	95
3.3.4. Programy .....	97
3.3.5. Konta użytkowników i Filtr rodzinny .....	98
3.3.6. Wygląd i personalizacja .....	101
3.3.7. Zegar, język i region .....	101
3.4. Wybrane narzędzia trybu poleceń do zarządzania składnikami systemu .....	103
3.4.1. NET.exe .....	103
3.4.2. SC.exe .....	106
<b>Rozdział 4. Zarządzanie dyskami i systemami plików w Windows 7 .....</b>	<b>109</b>
4.1. Narzędzia do zarządzania dyskami komputera .....	110
4.1.1. Przystawka Zarządzanie dyskami (DiskMgmt.msc) .....	110
4.1.2. Narzędzie trybu poleceń DiskPart.exe .....	111
4.2. Zaawansowane zarządzanie konfiguracją dysków komputera .....	112
4.2.1. Tworzenie partycji podstawowej NTFS dla aplikacji .....	113
4.2.2. Tworzenie partycji rozszerzonej FAT32 dla danych użytkowników .....	114
4.2.3. Formatowanie i kompresja woluminów NTFS a rozmiar jednostki alokacji .....	115
4.2.4. Konwertowanie woluminu FAT32 do systemu plików NTFS (Convert.exe) .....	118
4.3. Zarządzanie wydajnością dysków komputera .....	119
4.3.1. Defragmentacja dysku (DFRGUI.exe i Defrag.exe) .....	120
4.3.2. Oczyszczanie dysku (CleanMgr.exe) .....	123
4.4. Zaawansowane zagadnienia dotyczące dysków dynamicznych .....	129
4.4.1. Woluminy proste .....	130
4.4.2. Woluminy rozłożone .....	130
4.4.3. Woluminy paskowane (RAID-0) .....	131
4.4.4. Woluminy dublowane (RAID-1) .....	131
4.4.5. Woluminy paskowane z parzystością (RAID-5) .....	133
4.4.6. Zmniejszanie woluminu (DiskPart.exe) .....	134
4.4.7. Rozszerzanie woluminu (DiskMgmt.msc) .....	135
4.5. Tworzenie i usuwanie zestawu odpornego na uszkodzenia (RAID-1) .....	137
4.6. Zarządzanie przydziałami dysku .....	141
4.6.1. Włączanie przydziału dysku dla wszystkich użytkowników .....	142
4.6.2. Uzyskiwanie informacji o wpisach przydziału dysku .....	147
4.6.3. Tworzenie wpisu przydziału dysku dla wybranych użytkowników .....	148
4.6.4. Kompresja NTFS a przydziały dysku .....	150
4.7. Sprawdzanie dysków w poszukiwaniu błędów i uszkodzonych sektorów (ChkDsk.exe) .....	151
<b>Rozdział 5. Zarządzanie użytkownikami i grupami w systemie Windows 7 .....</b>	<b>155</b>
5.1. Narzędzia do zarządzania użytkownikami i grupami .....	156
5.1.1. Przystawka Użytkownicy i grupy lokalne (LUsrMgr.msc) .....	156
5.1.2. Panel Konta użytkowników i Filtr rodzinny .....	157
5.2. Istota kont użytkowników i grup oraz różnice pomiędzy nimi .....	157

5.3. Zabezpieczanie kont użytkowników i zarządzanie hasłami .....	159
5.3.1. Zabezpieczanie kont użytkowników (Whoami.exe) .....	159
5.3.2. Opcje zabezpieczeń kont użytkowników .....	160
5.3.3. Metody uwierzytelniania użytkowników .....	162
5.3.4. Zaawansowane zarządzanie zasadami haseł i blokady konta .....	162
5.4. Tworzenie lokalnych kont użytkowników i grup .....	171
5.4.1. Tworzenie nowego użytkownika i konfigurowanie opcji zabezpieczeń .....	171
5.4.2. Tworzenie nowej grupy i dołączanie członków grupy .....	172
5.5. Zarządzanie profilami użytkowników i konfigurowanie ich środowiska pracy .....	174
5.5.1. Zarządzanie profilami użytkowników .....	175
5.5.2. Lokalne a mobilne profile użytkowników .....	176
5.5.3. Zarządzanie właściwościami profilu lokalnego użytkownika .....	177
5.5.4. Systemowe zmienne środowiskowe .....	178

## **Rozdział 6. Zaawansowane zarządzanie folderami i plikami w systemie Windows 7 ..... 181**

6.1. Narzędzia do zarządzania certyfikatami EFS .....	182
6.1.1. Przystawka Certyfikaty (CertMgr.msc) .....	182
6.1.2. Narzędzie trybu poleceń Cipher.exe .....	183
6.2. System szyfrowania plików (EFS) .....	184
6.2.1. Istota i zasada działania systemu EFS .....	186
6.2.2. System EFS a szyfrowanie symetryczne i asymetryczne .....	188
6.2.3. System EFS a obsługa certyfikatów RSA i ECC .....	189
6.2.4. Konfigurowanie systemu EFS do obsługi certyfikatów ECC .....	189
6.2.5. Szyfrowanie pliku certyfikatem ECC i udostępnianie go użytkownikom .....	192
6.3. Zarządzanie certyfikatami EFS (ReKeyWiz.exe) .....	197
6.4. Zarządzanie kompresją dysków i danych .....	200
6.4.1. Typy kompresji .....	201
6.4.2. Kompresja NTFS a szyfrowanie EFS .....	202
6.4.3. Kompresja i dekompresja danych (Compact.exe i Expand.exe) .....	203

## **Rozdział 7. Zarządzanie sieciami TCP/IP w Windows 7 ..... 207**

7.1. Narzędzia do zarządzania ustawieniami sieci TCP/IP .....	208
7.1.1. Panel Centrum sieci i udostępniania .....	208
7.1.2. Panel Grupa domowa .....	210
7.1.3. Narzędzie trybu poleceń Netsh.exe .....	212
7.2. Narzędzia do zdalnego zarządzania komputerami .....	214
7.2.1. Narzędzie Podłączanie pulpitu zdalnego (MSTsc.exe) .....	214
7.2.2. Narzędzia administracji zdalnej serwera dla systemu Windows 7 (RSAT) .....	215
7.3. Zarządzanie lokalnymi ustawieniami sieci TCP/IP .....	217
7.3.1. Statyczna a dynamiczna adresacja sieci TCP/IP .....	217
7.3.2. Konfigurowanie zaawansowanych ustawień sieciowych .....	218
7.4. Windows 7 Professional a praca w grupie domowej .....	220
7.4.1. Testowanie lokalnych ustawień sieci TCP/IP (IPConfig.exe) .....	220
7.4.2. Dołączanie komputera do grupy domowej w trybie online .....	222
7.5. Windows 7 Professional a praca w domenie Active Directory .....	226
7.5.1. Dołączanie komputera do domeny Active Directory w trybie offline (DJoin.exe) .....	226
7.5.2. Przechowywanie poświadczeń kont domenowych .....	230
7.5.3. Zwalnianie i odświeżanie ustawień DHCP .....	232
7.5.4. Rejestrowanie i czyszczenie buforów DNS .....	233
7.6. Wybór poziomu uwierzytelniania DCOM a wydajność sieci (DCOMCnfg.exe) .....	235

7.7. Wybrane narzędzia do diagnozowania problemów sieciowych .....	239
7.7.1. Ping.exe .....	239
7.7.2. ARP.exe .....	240
7.7.3. NetStat.exe .....	242
7.7.4. Route.exe .....	244
<b>Rozdział 8. Zarządzanie bezpieczeństwem w Windows 7 .....</b>	<b>247</b>
8.1. Narzędzia do zarządzania bezpieczeństwem systemu i komputera .....	248
8.1.1. Panel Centrum akcji (WScUI.cpl) .....	248
8.1.2. Przystawka Zasady zabezpieczeń lokalnych (SecPol.msc) .....	248
8.1.3. Narzędzie Zabezpieczanie bazy danych kont systemu Windows (SysKey.exe) .....	249
8.2. Narzędzia do zarządzania bezpieczeństwem plików systemowych i sterowników .....	251
8.2.1. Menedżer weryfikatora sterowników (Verifier.exe) .....	252
8.2.2. Weryfikacja podpisu pliku (SigVerif.exe) .....	257
8.2.3. Kontroler zasobów systemu Windows (SFC.exe) .....	259
8.3. Wybrane metody zabezpieczania konfiguracji systemu .....	260
8.3.1. Stosowanie do logowania kart inteligentnych zamiast haseł .....	261
8.3.2. Wyłączenie nieużywanych usług systemowych .....	262
8.3.3. Wyłączenie udziałów domyślnych .....	265
8.3.4. Blokowanie komputera (TSDiscon.exe) .....	268
8.3.5. Przygotowanie procedury archiwizacji i odtwarzania danych (SDCLT.exe) .....	270
8.4. Zarządzanie inspekcją dotyczącą logowania .....	274
8.4.1. Konfigurowanie inspekcji zdarzeń logowania .....	275
8.4.2. Konfigurowanie inspekcji zdarzeń logowania na kontach .....	277
8.5. Zaawansowane konfigurowanie zabezpieczeń w Windows 7 .....	277
8.5.1. Logowanie interakcyjne: tytuł komunikatu dla użytkowników próbujących się zalogować .....	277
8.5.2. Logowanie interakcyjne: tekst komunikatu dla użytkowników próbujących się zalogować .....	278
8.5.3. Klient sieci Microsoft: podpisuj cyfrowo komunikację (zawsze) .....	278
8.5.4. Kryptografia systemu: wymuś mocną ochronę klucza dla kluczy użytkowników przechowywanych na komputerze .....	279
8.5.5. Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika .....	281
8.5.6. Logowanie interakcyjne: liczba pośrednich zalogowań do zbuforowania (w przypadku niedostępności kontrolera domeny) .....	281
8.5.7. Logowanie interakcyjne: monituj użytkownika o zmianę hasła przed jego wygaśnięciem .....	282
8.5.8. Zamknięcie: wyczyść plik stronicowania pamięci wirtualnej .....	283
<b>Rozdział 9. Zarządzanie wydajnością i optymalizacja systemu Windows 7 .....</b>	<b>285</b>
9.1. Zaawansowane narzędzia do monitorowania aktywności i wydajności komputera .....	286
9.1.1. Monitor wydajności (PerfMon.exe) .....	286
9.1.2. Monitor zasobów (ResMon.exe) .....	287
9.1.3. Monitor niezawodności .....	294
9.2. Tworzenie szczegółowego raportu dotyczącego „kondycji systemu” .....	297
9.3. Zarządzanie aplikacjami, procesami i wydajnością systemu (TaskMgr.exe) .....	301
9.4. Zaawansowane zarządzanie właściwościami systemu (SystemPropertiesAdvanced.exe) .....	308
9.4.1. Zarządzanie wydajnością aplikacji .....	309
9.4.2. Zarządzanie pamięcią wirtualną .....	311
9.4.3. Zarządzanie uruchamianiem i odzyskiwaniem systemu .....	314

---

9.5. Monitorowanie i zaawansowane dostrajanie wydajności systemu .....	316
9.5.1. Monitorowanie wydajności i wykorzystania pamięci .....	318
9.5.2. Monitorowanie wydajności i wykorzystania procesora .....	319
9.5.3. Monitorowanie wydajności i wykorzystania dysków fizycznych .....	321
9.5.4. Monitorowanie wydajności i wykorzystania interfejsu sieciowego .....	321
9.6. Wyszukiwanie problemów związanych z systemem operacyjnym i aplikacjami .....	323
9.7. Wieloprocusorowość a rzeczywista wydajność systemu i koligacja procesów .....	324
9.8. Zaawansowane opcje rozruchu systemu w przypadku awarii .....	327
9.8.1. Opcja Napraw komputer .....	327
9.8.2. Opcja Tryb awaryjny .....	334
9.8.3. Opcja Włącz rejestrowanie rozruchu .....	335
9.8.4. Opcja Ostatnia znana dobra konfiguracja (zaawansowane) .....	336
9.8.5. Opcja Wyłącz automatyczne ponowne uruchamianie komputera po błędzie systemu .....	336
<b>Dodatek A Nowe skróty klawiaturowe w systemie Windows 7 Professional .....</b>	<b>339</b>
<b>Dodatek B Konsole systemu Windows 7 Professional .....</b>	<b>341</b>
<b>Bibliografia .....</b>	<b>343</b>
<b>Skorowidz .....</b>	<b>347</b>

## 8.4.2. Konfigurowanie inspekcji zdarzeń logowania na kontach

Inspekcja zdarzeń logowania na kontach rejestruje zdarzenia logowania i wylogowywania użytkowników na komputerze pracującym pod kontrolą systemu Windows 7 Professional, a wyniki jej pracy zapisywane są w dzienniku systemowym *Zabezpieczenia*.

Aby skonfigurować inspekcję zdarzeń logowania na kontach w komputerze pracującym pod kontrolą systemu Windows 7 Professional, należy z poziomu przystawki *Edytor lokalnych zasad grupy* przejść do wspomnianej wcześniej gałęzi oraz wykonać (jako lokalny administrator) przedstawione poniżej kroki.

1. Zaznaczamy w środkowym panelu zasadę *Przeprowadź inspekcję zdarzeń logowania na kontach (Audit Account Logon Events)*.
2. Z menu *Akcja (Action)* wybieramy polecenie *Właściwości (Properties)*.
3. W oknie przedstawionym na rysunku 8.27 zaznaczamy opcję *Niepowodzenie (Failure)* i klikamy przycisk *OK*.
4. Zamykamy przystawkę *Edytor lokalnych zasad grupy*.

Ustawienie zabezpieczeń *Przeprowadź inspekcję zdarzeń logowania na kontach* pozwala określić (zgodnie z rysunkiem 8.27), czy każda weryfikacja poświadczeń konta na lokalnym komputerze (aktywna opcja *Niepowodzenie [Failure]*) ma być poddawana inspekcji w systemie Windows 7 Professional.

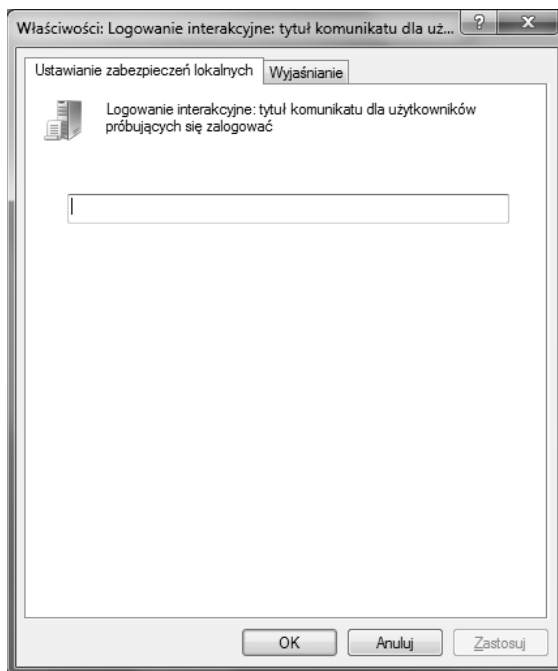
## 8.5. Zaawansowane konfigurowanie zabezpieczeń w Windows 7

Zaawansowane konfigurowanie zabezpieczeń w systemie Windows 7 Professional można przeprowadzić z poziomu przystawki *Edytor lokalnych zasad grupy* w gałęzi *Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Opcje zabezpieczeń (Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options)*. W powyższej lokalizacji można znaleźć szereg przydatnych ustawień zabezpieczeń. Niektóre z nich zostały przedstawione w dalszej części książki.

### 8.5.1. Logowanie interakcyjne: tytuł komunikatu dla użytkowników próbujących się zalogować

Ustawienie zabezpieczeń lokalnych w postaci zasady *Logowanie interakcyjne: tytuł komunikatu dla użytkowników próbujących się zalogować (Interactive logon: Message title for users attempting to log on)*, które zostało pokazane na rysunku 8.28, zezwala na określenie tytułu wypisywanego użytkownikowi podczas logowania się — zanim zostanie wyświetlony ekran logowania systemu Windows 7 Professional.

**Rysunek 8.28.**  
Okno dialogowe  
Właściwości:  
Logowanie  
interakcyjne:  
tytuł komunikatu  
dla użytkowników  
próbujących się  
zalogować



### 8.5.2. Logowanie interakcyjne: tekst komunikatu dla użytkowników próbujących się zalogować

Ustawienie zabezpieczeń lokalnych w postaci zasady *Logowanie interakcyjne: treść komunikatu dla użytkowników próbujących się zalogować* (*Interactive logon: Message text for users attempting to log on*), które zostało pokazane na rysunku 8.29, zezwala na określenie treści komunikatu wyświetlanego każdemu użytkownikowi podczas logowania się — zanim zostanie wyświetlony ekran logowania systemu Windows 7 Professional. To rozwiązanie jest często wykorzystywane w dużych przedsiębiorstwach oraz organizacjach z przyczyn prawnych, np. w celu ostrzeżenia użytkowników o konsekwencjach nieprawidłowego wykorzystania informacji firmowych lub możliwości poddania inspekcji czynności, które użytkownicy wykonują na komputerze.

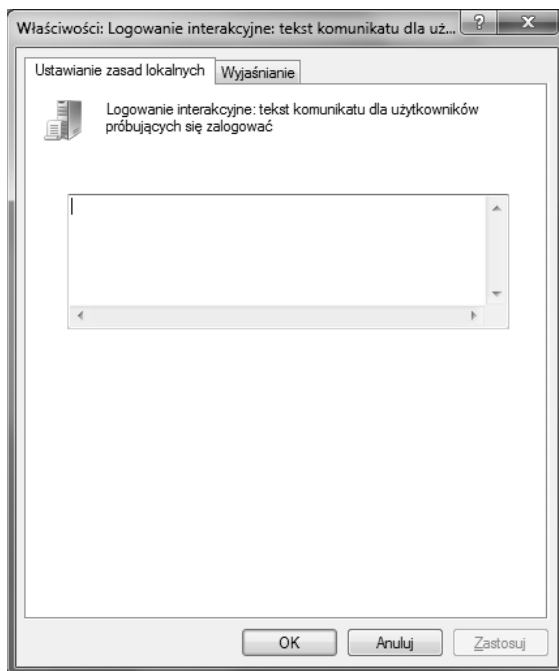
### 8.5.3. Klient sieci Microsoft: podpisuj cyfrowo komunikację (zawsze)

Wszystkie edycje systemu Windows 7 obsługują do 20 połączeń z wykorzystaniem protokołu o nazwie *Blok komunikatów serwera* (*Server Message Block*) w wersji 2.0. Protokół *SMB* jest podstawą mechanizmu udostępniania danych i drukarek w systemach Windows 7 Professional oraz operacji sieciowych, takich jak np. zdalne administrowanie.



**Rysunek 8.29.**

Okno dialogowe  
Właściwości:  
Logowanie  
interakcyjne:  
treść komunikatu  
dla użytkowników  
próbujących się  
zalogować

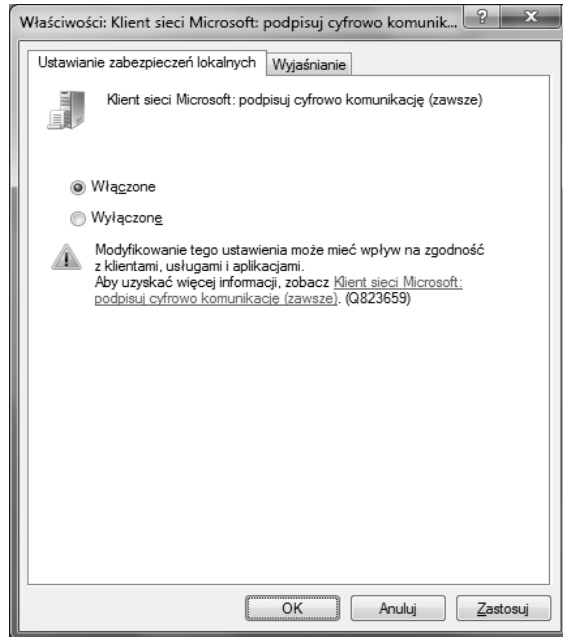


Aby zapobiec atakom pochodzącym wnętrza sieci, które polegają np. na modyfikowaniu transmitowanych pakietów *SMB*, wspomniany wcześniej protokół *SMB* obsługuje cyfrowe podpisywanie tych pakietów. Służy do tego zasada ustawienia zabezpieczeń lokalnych o nazwie *Klient sieci Microsoft: podpisuj cyfrowo komunikację (zawsze)* (*Microsoft network client: Digitally sign communications (always)*), której dwie opcje zostały pokazane na rysunku 8.30. Po włączeniu tego ustawienia pakiety *SMB* będą podpisywane cyfrowo przez system Windows 7 Professional. Warto wiedzieć, że klient sieci firmy Microsoft nie będzie mógł komunikować się np. z serwerem sieci firmy Microsoft, dopóki serwer ten nie zgodzi się na podpisywanie pakietów *SMB*.

#### 8.5.4. Kryptografia systemu: wymuś mocną ochronę klucza dla kluczy użytkowników przechowywanych na komputerze

Ustawienie zabezpieczeń lokalnych w postaci zasady *Kryptografia systemu: wymuś mocną ochronę klucza dla kluczy użytkowników przechowywanych na komputerze* (*System cryptography: Force strong key protection for user keys stored on the computer*), której jedna z opcji została przedstawiona na rysunku 8.31, określa, czy użycie kluczy prywatnych użytkowników wymaga podania hasła. Dostępne są takie opcje jak:

- ♦ *Wprowadzenie danych przez użytkownika nie jest wymagane przy zachowaniu i używaniu nowych kluczy (User input is not required when new keys are stored and used),*

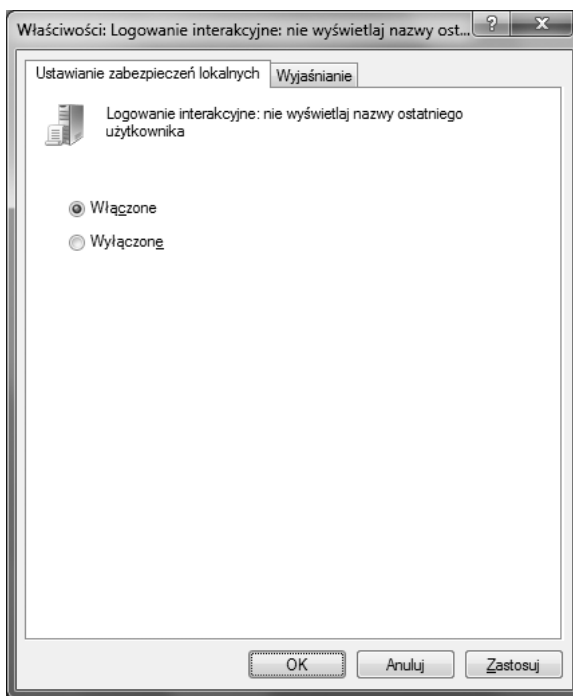
**Rysunek 8.30.***Okno dialogowe**Właściwości:**Klient sieci Microsoft:  
podpisuj cyfrowo  
komunikację (zawsze)***Rysunek 8.31.***Okno dialogowe**Właściwości:**Kryptografia systemu:  
wymuś mocną ochronę  
klucza dla kluczy  
użytkowników  
przechowywanych  
na komputerze*

- ◆ *Użytkownik jest monitowany przy pierwszym użyciu klucza (User is prompted when the key is first used),*
- ◆ *Użytkownik musi wprowadzić hasło za każdym razem, gdy używa klucza (User must enter a password each time they use a key).*

### 8.5.5. Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika

Ustawienie zabezpieczeń lokalnych w postaci zasady *Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika* (*Interactive logon: Do not display last user name*), które zostało przedstawione na rysunku 8.32, określa, czy na ekranie logowania systemu Windows 7 Professional będzie wyświetlana nazwa użytkownika, który ostatnio zalogował się na komputerze. Jej brak nie pozwala intruzowi poznać nazwy użytkownika, który ma konto w systemie. Potencjalny intruz nie tylko będzie musiał odkryć nazwę użytkownika, ale i jego hasło, co dodatkowo chroni dostęp do systemu Windows 7 Professional.

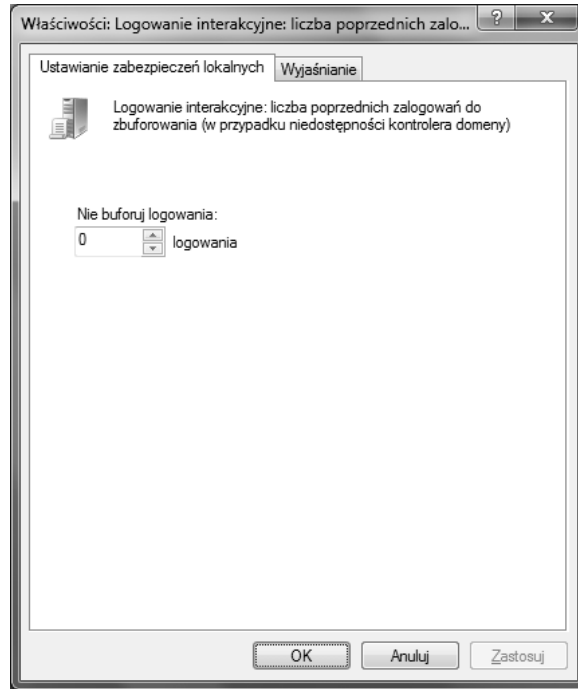
**Rysunek 8.32.**  
*Okno dialogowe  
Właściwości:  
Logowanie  
interakcyjne:  
nie wyświetlaj  
nazwy ostatniego  
użytkownika*



### 8.5.6. Logowanie interakcyjne: liczba pośrednich zalogowań do zbuforowania (w przypadku niedostępności kontrolera domeny)

Ustawienie zabezpieczeń lokalnych w postaci zasady *Logowanie interakcyjne: liczba pośrednich zalogowań do zbuforowania (w przypadku niedostępności kontrolera domeny)* (*Interactive logon: Numbers of previous logons to cache (in case domain controller is not available)*), które zostało pokazane na rysunku 8.33, określa, czy będzie możliwe pracowanie na kontach domenowych przy jednoczesnym braku dostępu do jakiegokolwiek

**Rysunek 8.33.**  
Okno dialogowe  
Właściwości:  
Logowanie  
interakcyjne:  
liczba pośrednich  
zalogowań  
do zbuforowania  
(w przypadku  
nieдоступności  
kontrolera domeny)



kontrolera domeny. Ustawienie w tej zasadzie wartości 0 spowoduje wyłączenie buforowania lokalnego kont domenowych, a tym samym niemożność pracy na tego typu koncie przy braku możliwości skontaktowania się z kontrolerem domeny.

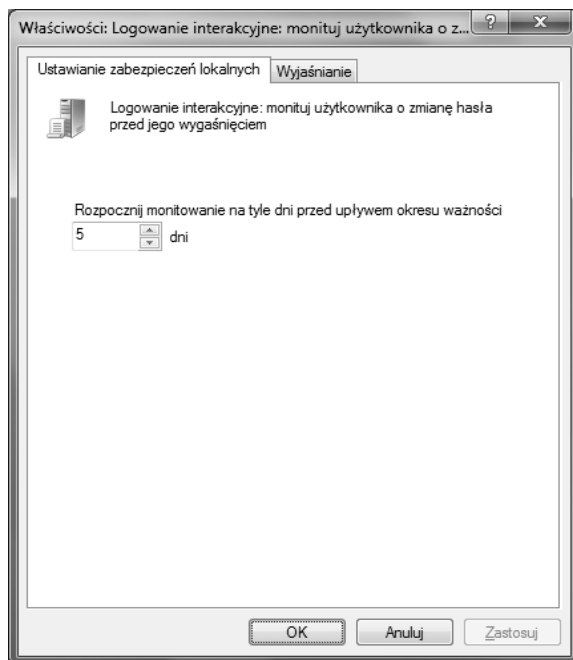


Wskazówka

Alternatywna metoda zmiany domyślnej wartości poświadczeń kont domenowych przechowywanych w buforze lokalnego komputera została zaprezentowana w rozdziale 7. tej publikacji i polegała na edycji rejestru systemu Windows, a dokładniej ciągu *CachedLogonsCount* typu *REG\_SZ* znajdującego się w kluczu *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon*.

### 8.5.7. Logowanie interakcyjne: monituj użytkownika o zmianę hasła przed jego wygaśnięciem

Ustawienie zabezpieczeń lokalnych w postaci zasady *Logowanie interakcyjne: monituj użytkownika o zmianę hasła przed jego wygaśnięciem* (*Interactive logon: Prompt user to change password before expiration*), które zostało przedstawione na rysunku 8.34, określa, z jakim wyprzedzeniem (w dniach) użytkownicy będą ostrzegani o wygaśnięciu hasła dostępowego. Dzięki temu będą mieli czas na przygotowanie tzw. silnego hasła. W systemie Windows 7 Professional jest to okres 14 dni. Można go zmienić na inny, np. 5 dni.

**Rysunek 8.34.***Okno dialogowe**Właściwości:**Logowanie**interakcyjne:**monituj użytkownika**o zmianę hasła przed**jego wygaśnięciem*

## 8.5.8. Zamknięcie: wyczyść plik stronicowania pamięci wirtualnej

Plik stronicowania pamięci wirtualnej *pagefile.sys* używany jest przez funkcje obsługi pamięci wirtualnej do zapisywania na dysku twardym nieużywanych stron pamięci fizycznej. W poprawnie działającym systemie Windows 7 Professional plik ten jest chroniony oraz otwierany wyłącznie przez system operacyjny. Jednakże w systemach, w których została skonfigurowana możliwość rozruchu innych systemów operacyjnych, może być konieczne zagwarantowanie, że plik stronicowania jest czyszczony podczas zamykania systemu. Tego typu zabieg ma na celu głównie uniemożliwienie dostępu nieautoryzowanym użytkownikom (intruzom) do poufnych informacji z pamięci procesów, które mogły zostać zapisane w pliku stronicowania na dysku twardym, nawet wtedy, kiedy uda im się uzyskać bezpośredni dostęp do tego systemowego pliku.

**Uwaga**

*Plik stronicowania* to obszar dysku twardego używany przez system Windows 7 Professional tak, jakby była to pamięć fizyczna.

Ustawienie zabezpieczeń lokalnych w postaci zasady o nazwie *Zamknięcie: wyczyść plik stronicowania pamięci wirtualnej* (*Shutdown: Clear virtual memory pagefile*), które zostało pokazane na rysunku 8.35, określa, czy plik stronicowania pamięci wirtualnej będzie czyszczony podczas zamykania systemu Windows 7 Professional. Włączenie tej zasady powoduje czyszczenie systemowego pliku stronicowania pamięci wirtualnej podczas zamykania systemu operacyjnego, przez co samo jego zamykanie wydłuża się nieznacznie.

**Rysunek 8.35.**  
*Okno dialogowe  
Właściwości:  
Zamknięcie:  
wyczyść plik  
stronicowania  
pamięci*

