

Systemy operacyjne 1

Spis treści

Konta użytkowników i grup w systemie Windows	3
Rodzaje kont	3
Grupy domyślne	3
Konwencje nazewnicze	4
Tworzenie konta Microsoft	5
Tworzenie konta lokalnego	6
Przystawka Użytkownicy i grupy lokalne (LUsrMgr.msc)	6
Dodawanie użytkownika do grupy	9
Foldery macierzyste	10
Uruchamianie aplikacji jako inny użytkownik	11
Ekran startowy – Konta użytkowników	12
Ekran startowy – Ustawienia konta	14
Aplikacja NET.EXE	16
Zadania	18
Uprawnienia	20
Mechanizm uprawnień w Windows	20
Standardowe prawa dostępu do folderów	20
Uprawnienia do plików	21
Lista kontroli dostępu	21
Uprawnienia wielokrotne	22
Kumulowanie uprawnień	22
Nadpisywanie uprawnień	22
Uprawnienie Odmawiaj	22
Dziedziczenie uprawnień	23
Przypisywanie i modyfikowanie uprawnień	23
Wyłączanie dziedziczenia uprawnień	24
Uprawnienia specjalne	25
TABELA	25
Uprawnienie Zmiana uprawnień	26

Uprawnienie Przejęcie na własność	26
Przypisywanie specjalnych uprawnień	27
Kopiowanie i przenoszenie plików i folderów	29
Kopiowanie zasobów	29
Przenoszenie zasobów	30
Zadania.....	31
Udostępnianie plików i folderów	32
Tworzenie udziału	32
Zadania.....	34

Konta użytkowników i grup w systemie Windows

Rodzaje kont

Konta użytkowników to podstawowe podmioty zabezpieczeń w systemie Windows, pozwalające użytkownikom na zalogowanie się i uzyskanie dostępu do zasobów, np. plików czy folderów. Przeznaczone są dla pojedynczych użytkowników, a przypisane im uprawnienia są sprawdzane w chwili uzyskiwania przez nich dostępu do tych zasobów.

Konta grup (grupy) ułatwiają zarządzanie zasobami dla wielu użytkowników równocześnie. Nie umożliwiają np. zalogowania się do systemu bez podania konta użytkownika i skojarzonego z nim hasła dostępowego.

Wśród kont użytkowników występują:

- **lokalne konta użytkowników** — to konta, które zostały zdefiniowane na lokalnym komputerze pracującym pod kontrolą systemu Windows; konta te zapewniają dostęp tylko do zasobów tego komputera, na którym zostały utworzone (konta tego typu można tworzyć np. z poziomu konsoli **Użytkownicy i grupy lokalne** – LusrMgr.msc),
- **domenowe konta użytkowników** — to konta zdefiniowane w usłudze katalogowej Active Directory; za ich pomocą użytkownicy domeny sieciowej Active Directory mogą uzyskiwać dostęp do komputerów w całej domenie; konta są przechowywane na komputerze będącym kontrolerem domeny np. Windows 2012 Serwer z usługą Active Directory i tylko na nim można je zakładać.
- **konta wbudowane** — Są to konta o nazwach Gość i Administrator, tworzone podczas instalacji systemu i dostępne z poziomu wspomnianej wcześniej konsoli **Użytkownicy i grupy lokalne**.
 - Konto **Administrator** umożliwia wykonanie wszelkich zadań (w tym zadań administracyjnych) takich jak m.in.: wyłączanie systemu, zakładanie i zarządzanie kontami użytkowników, itp.
 - Konto **Gość** posiada minimalny zestaw uprawnień i pozwala użytkownikowi na zalogowanie się do komputera nawet wtedy, jeśli nie posiada na nim konta. Konto to należy uaktywniać tylko w specyficznych warunkach, ponieważ jego istnienie powoduje, że dostęp do komputera ma praktycznie każdy.

Wbudowanych grup, podobnie jak i wbudowanych lokalnych kont użytkowników, nie można usuwać. Można natomiast zmieniać ich właściwości.

Grupy domyślne

W trakcie instalacji systemu Windows tworzonych jest kilkanaście grup domyślnych. Umieszcza się w nich konta użytkowników, co pozwala określić odpowiednie

uprawnienia do wykonywania określonych zadań dla danego konta. Przykładowe grupy domyślnie to:

Administratorzy (Administrators) użytkownicy mający

pełny dostęp do komputera

Operatorzy kopii zapasowych (Backup Operators) użytkownicy mający uprawnienia do wykonywania kopii zapasowych za pomocą służącego do tego celu oprogramowania.

Goście (Guests) nie mogą instalować programów i wprowadzać innych zmian w systemie. Mogą natomiast korzystać z komputera i zapisywać pliki.

Użytkownicy zaawansowani (Power Users) użytkownicy mający prawo do instalacji programów i modyfikacji konfiguracji systemu. Użytkownicy ci nie mają jednak dostępu do plików innych użytkowników. Są uwzględnieni dla kompatybilności z poprzednimi wersjami systemu.

Replikator (Replicator) grupa obsługi replikacji

plików w domenie

Użytkownicy (Users) podobnie jak Goście, posiadają oni minimalne uprawnienia i nie mogą modyfikować konfiguracji systemu; nie mogą przeprowadzać przypadkowych ani celowych zmian na poziomie całego systemu i mogą uruchamiać większości aplikacji.

Inne grupy wbudowane Windows to:

Administratorzy funkcji Hyper-V, Czytelnicy dzienników zdarzeń IIS_IUSRS, Operatorzy konfiguracji sieci, Operatorzy kryptograficzni, Operatorzy kontroli dostępu, Użytkownicy DCOM, Użytkownicy dzienników wydajności, Użytkownicy monitora wydajności, Użytkownicy pulpitu zdalnego, Użytkownicy zarządzania zdalnego, HomeUsers, WinRMRemoteWMIUsers_.

Opisy tych grup znajdują się w oknie **Użytkownicy i grupy lokalne\Grupy**.

Grupy te umożliwiają wykonanie określonych zadań, do których ich członkowie mają (lub nie) prawo. Grupy wbudowane nie zapewniają jednak specyficznych uprawnień do plików i katalogów systemu plików.

Konwencje nazewnicze

Konwencje nazewnicze określają w jaki sposób konto użytkownika lub grupy będzie identyfikowane w systemie. Przyjęcie pewnych zasad pozwoli w łatwiejszy sposób tworzyć nowe konta, a później nimi zarządzać. W przypadku kont użytkownika warto stosować poniższe zasady:

- Nazwa użytkownika może zawierać maksymalnie 20 wielkich lub małych znaków (można wpisać więcej, ale system Windows rozpoznaje tylko 20 pierwszych znaków), z wyjątkiem: "\/:; = , + *?<>

- Nazwa konta musi być unikalna na komputerze, na którym to konto jest tworzone. W przypadku kont domenowych, nazwa konta musi być unikalna w całej domenie, w której to konto ma zostać założone.
- Nazwa użytkownika może być dowolną kombinacją znaków specjalnych i alfanumerycznych. Windows nie rozróżnia wielkość liter, z których składa się nazwa użytkownika (jednak zachowuje wielkość liter tak jak wprowadził je użytkownik).
- W systemie Windows do logowania można używać także własnego adresu pocztowego skojarzonego z kontem Microsoft. Jeśli nie podano konwencjonalnej nazwy użytkownika system tworzy nazwę korzystając z loginu wprowadzonego w adresie pocztowym.
- W przypadku grup obowiązują bardzo podobne zasady, jeśli chodzi o nazewnictwo. Przedstawione są one poniżej:
- Nazwa grupy powinna składać się z maksymalnie 256 znaków. Dopuszczalne są wszystkie znaki z wyjątkiem: "/\.;=,+*?<>
- Nazwa grupy musi różnić się od nazw innych grup lokalnych oraz kont użytkowników dostępnych w systemie.

Tworzenie konta Microsoft

Konto Microsoft to adres e-mail i hasło używane do logowania się do systemu Windows. Można użyć dowolnego adresu e-mail, ale najlepiej wybrać adres już używany do komunikacji ze znajomymi i do logowania się do ulubionych witryn sieci Web. Logując się do komputera przy użyciu konta Microsoft, łączysz go z osobami, plikami i urządzeniami, które są dla Ciebie istotne. (W razie braku adresu e-mail można go bezpłatnie uzyskać od firmy Microsoft).

Po zalogowaniu się na koncie Microsoft komputer jest połączony z magazynem w chmurze w trybie online. Ma to następujące znaczenie:

- Ustawienia osobiste są synchronizowane ze wszystkimi komputerami z systemami Windows, do których logujemy się przy użyciu tego konta. Obejmuje to motywy, preferencje językowe, elementy dodane do ulubionych w przeglądarce i większość aplikacji.
- Aplikacje można uzyskać w Sklepie Windows i korzystać z nich na maksymalnie pięciu komputerach z systemami Windows.
- Informacje o kontaktach i statusach znajomych są aktualizowane na bieżąco na podstawie danych z miejsc takich jak witryna Outlook.com i usługi Facebook, Twitter oraz LinkedIn.
- Można korzystać ze swoich zdjęć, dokumentów i innych plików (oraz je udostępniać) z takich miejsc, jak system OneDrive oraz usługi Facebook i Flickr. [Aby utworzyć konto Microsoft](#)

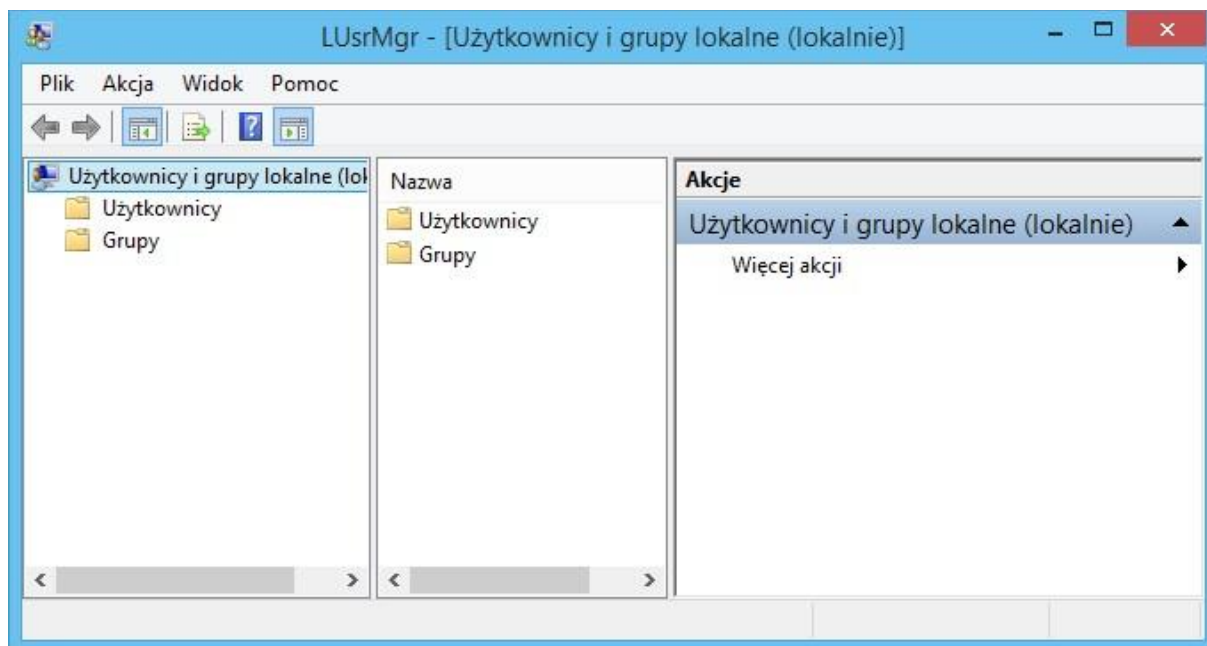
- Szybko przesunąć od prawej krawędzi do środka ekranu, nacisnąć panel Ustawienia, a następnie nacisnąć pozycję Zmień ustawienia komputera. (Jeśli używasz myszy, wskaż prawy dolny róg ekranu, przesunąć wskaźnik myszy w górę, kliknąć panel Ustawienia, a następnie kliknąć pozycję Zmień ustawienia komputera).
- Naciśnij lub kliknij pozycję Konta, a następnie naciśnij lub kliknij pozycję Inne konta.
- Naciśnij lub kliknij pozycję Dodaj konto.
- Wprowadź informacje o koncie umożliwiające danej osobie logowanie się do systemu Windows. Można to zrobić na cztery sposoby:
 - Jeśli dodawana osoba ma już konto Microsoft, wprowadź je teraz.
 - Jeśli dodawana osoba nie ma konta Microsoft, możesz je utworzyć przy użyciu adresu e-mail tej osoby. Wprowadź adres e-mail najczęściej używany przez tę osobę.
 - Jeśli dodawana osoba nie ma adresu e-mail, naciśnij lub kliknij pozycję Utwórz konto, aby otrzymać nowy adres e-mail. Jest to bezpłatne.
 - Jeśli dodawana osoba to dziecko, naciśnij lub kliknij pozycję Dodaj konto dziecka.
- Dokończ konfigurowanie konta, wykonując wyświetlane instrukcje.

Tworzenie konta lokalnego

Wykonuje się je zwykle jedną z 3 metod: poprzez konsolę **Użytkownicy i grupy lokalne**, moduł **Konta i Bezpieczeństwo rodzinne** lub aplikację konsolową net.exe.

Przystawka Użytkownicy i grupy lokalne (LUsrMgr.msc)

Konsolę Użytkownicy uruchamia się z linii poleceń (klawisze Windows+R), w okienku konsoli systemu, także poprzez program Windows PowerShell za pomocą komendy **LUsrMgr.msc**, lub jako „Panel Sterowania\ Narzędzia Administracyjne\ Zarządzanie komputerem\ **Użytkownicy i grupy lokalne**”. Jest to podstawowe miejsce do administrowania i zarządzania kontami użytkowników oraz grupami lokalnymi. Domyślnie konsola **Użytkownicy i grupy lokalne** zawiera (rys.) dwa obiekty: Użytkownicy i Grupy.




Przystawka Użytkownicy i grupy lokalne

Za pomocą przystawki **Użytkownicy i grupy lokalne** można:

- tworzyć nowych użytkowników i usuwać istniejących, tworzyć nowe grupy użytkowników i usuwać istniejące,
- zarządzać kontami użytkowników i grup użytkowników.

Tworzenie nowego użytkownika z poziomu tej konsoli (rysunek okna) wymaga wykonania przedstawionych poniżej kroków:

- zaznaczenia obiektu **Użytkownicy**,
- wybrania z menu **Akcja** opcji **Nowy użytkownik...**,
- wypełnienia przynajmniej trzech pól: **Nazwa użytkownika**, **Hasło** i **Powtórz hasło**,  zatwierdzenia akcji przyciskami **Utwórz**, a następnie **Zamknij**.

Po utworzeniu konta użytkownika można edytować jego właściwości. Za pomocą 3 zakładek w oknie dialogowym **Właściwości** można m.in. przydzielać użytkownika do odpowiednich grup, konfigurować jego profil czy środowisko pracy i wykonywać wiele innych czynności.

Wyświetlone okno **Właściwości** zawiera zakładki **Ogólne** z opcjami identycznymi jak przy zakładaniu konta, zakładkę **Członek grupy** z grupami, do których należy dane konto, oraz **Profil** z ustawieniami profilu danego użytkownika (Rysunek). Nazwę konta można dowolnie zmieniać i nie ma to wpływu na jego uprawnienia i logowanie. Wynika to z faktu, iż w systemie Windows konto jest identyfikowane w oparciu o identyfikator zabezpieczeń (SD) - Security ID), a nie o nazwę. Podobnie identyfikowane są grupy. Jeżeli więc konto zostanie usunięte, a następnie utworzone ponownie pod tą samą nazwą, zostanie mu przypisany całkowicie nowy numer SID, a wszystkie związane z tym kontem uprawnienia będzie trzeba ustawić na nowo.

Aby utworzyć nową grupę, należy kliknąć prawym przyciskiem na pozycji **Grupy** i wybrać polecenie **Nowa grupa**. W oknie dialogowym **Nowa grupa** (Rysunek) dostępne są następujące opcje:

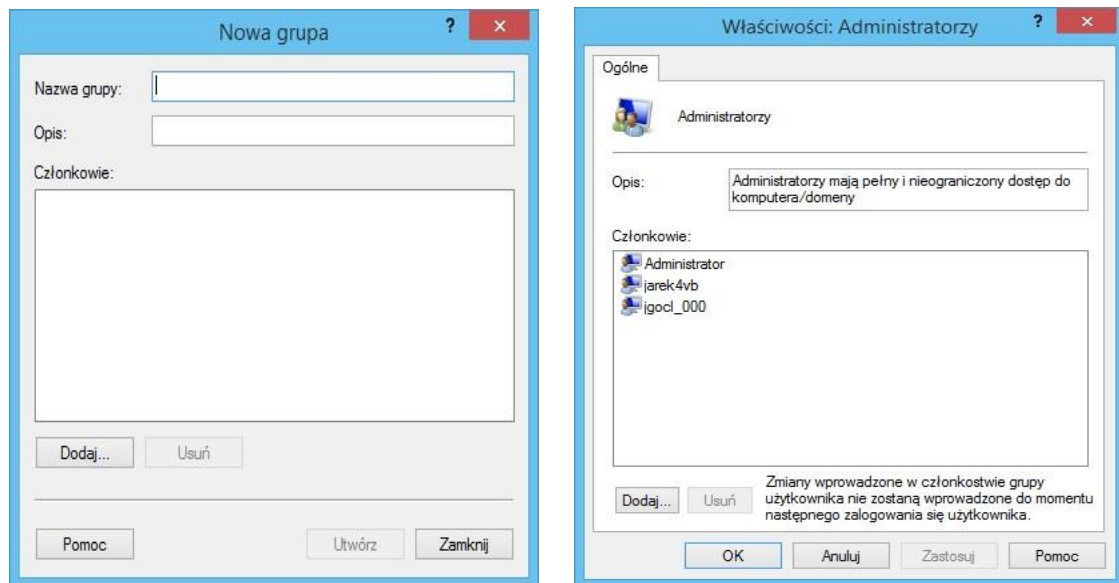
Nazwa grupy nazwa grupy lokalnej. Nazwy grup wbudowanych oraz już istniejących w systemie można zmieniać.

Opis opis grupy lokalnej.

Członkowie lista wszystkich członków, należących do danej grupy.

Dodaj i Usuń przyciski umożliwiające odpowiednio przypisanie nowych członków do grupy lub ich z niej usunięcie

Utwórz przycisk służący do utworzenia grupy.

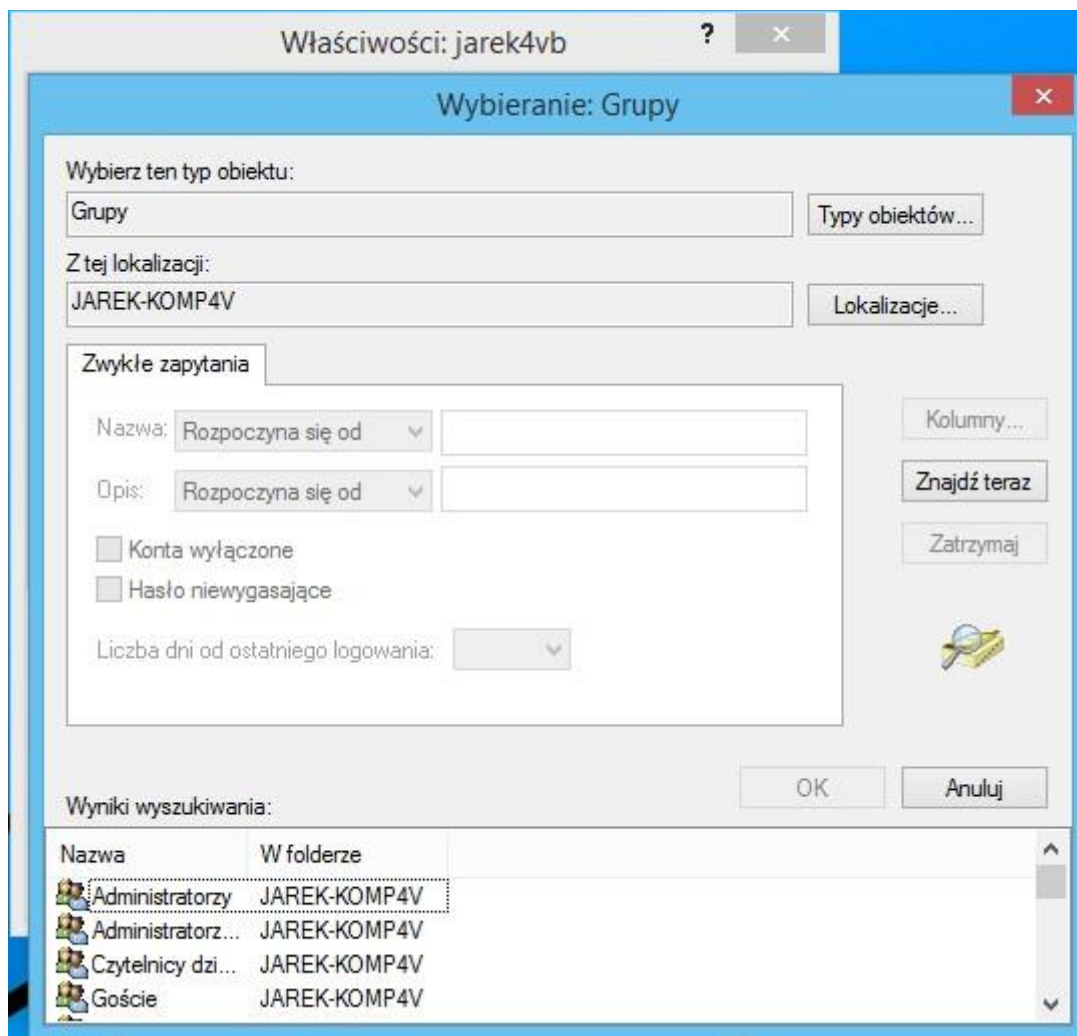


Do grup możemy dodawać nie tylko użytkowników, ale również inne grupy. Tworzenie użytkowników i grup domenowych wymaga działania usługi sieciowej Active Directory.

Dodawanie użytkownika do grupy

Przystawka **Użytkownicy i grupy lokalne** pozwala na dodanie użytkownika do grupy lokalnej. Zadanie to można zrealizować, albo w trakcie zakładanie konta nowej grupy, albo dodać użytkownika do grupy już istniejącej. Tę drugą możliwość można zrealizować na dwa sposoby:

- W pierwszym kroku należy rozwinąć gałąź **Użytkownicy**. Z wyświetlonej listy należy wybrać użytkownika, którego chcemy przypisać do grupy i wyświetlić dla niego okno **Właściwości**. W oknie tym należy wybrać zakładkę **Członek grupy**. Następnie nacisnąć przycisk **Dodaj**. Spowoduje to wyświetlenie okna **Wybieranie: Grupy**. Teraz należy wybrać przycisk **Zaawansowane**. W nowym oknie należy kliknąć na przycisk **Znajdź** teraz i na dole wybrać grupę. Na koniec należy kliknąć przycisk **OK** i potem **OK**. Użytkownik może należeć do dowolnej liczby grup, należy więc dodać tyle grup ile jest potrzebnych. Po kliknięciu przycisku **OK** dane konto staje się członkiem wybranych grup.
- W pierwszym kroku należy rozwinąć gałąź **Grupy**. Z wyświetlonej listy należy wybrać grupę, do której chcemy przypisać użytkownika i wyświetlić dla niej okno **Właściwości**. W oknie tym należy kliknąć przycisk **Dodaj** i wybrać odpowiedniego użytkownika lub grupę wyszukując ich w systemie w analogiczny sposób, co grupy (jak opisano w poprzednim punkcie). Następnie należy nacisnąć przycisk **OK**. Wybrany użytkownik zostanie wówczas przypisany do grupy.



Przypisanie użytkownika do grupy

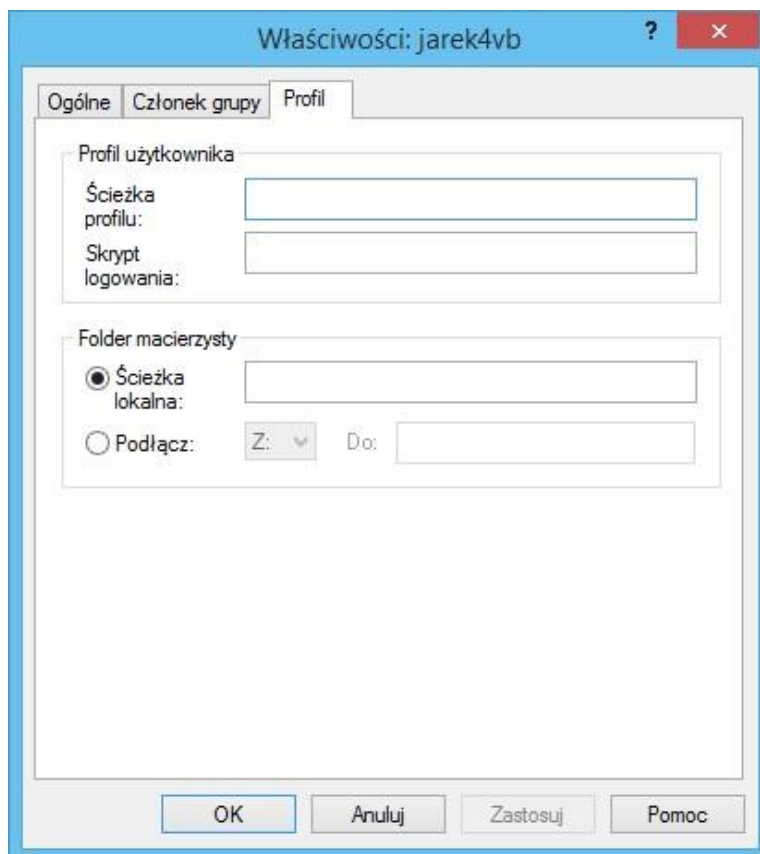
Foldery macierzyste

Folder macierzysty jest to folder użytkownika, który zawiera tylko jego własne dane. Jest to obszar przydzielony użytkownikowi, w którym może on przechowywać swoje własne pliki. Rozwiązanie takie umożliwia użytkownikowi przechowywanie swoich danych w pojedynczej, centralnej lokalizacji. Foldery macierzyste można umieścić na serwerze sieciowym. Foldery takie posiadają kilka korzyści:

- Uruchamiane programy, jeśli tego wymagają, używają folderu macierzystego jako własnego katalogu domyślnego
- Użytkownik może przydzielić uprawnienia dostępu do własnego folderu macierzystego.
- Do folderu macierzystego można przypisać odpowiednią literą napędu. Znacząco ułatwia to proces przechowywania danych, które są zawsze gromadzone w tym samym miejscu.

Aby ustawić odpowiedni folder należy wywołać okno **Właściwości** dla wybranego konta i wybrać zakładkę **Profil** (Rysunek). W obszarze **Folder macierzysty** należy wpisać ich położenie, aby utworzyć miejsce folderów macierzystych, stosując:

- Ścieżkę sieciową, np. \\nazwa_komputera\użytkownicy\Jan_K
- Ścieżkę lokalną np. c:\users\Jan_K
- Podstawienie zmiennych np. %username% zamiast nazwy użytkownika:
[\\Komputery\users\%username%](#)



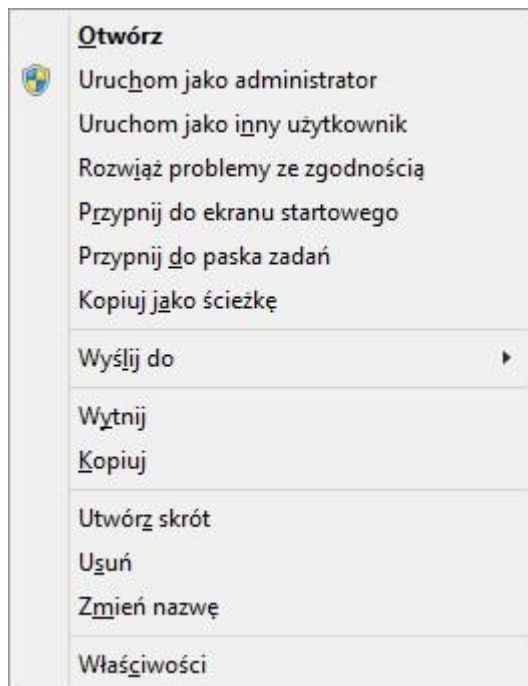
Uruchamianie aplikacji jako inny użytkownik

Konto **Administrator** w systemie Windows powinno być stosowane tylko do instalacji nowego sprzętu i oprogramowania oraz do przeprowadzania napraw systemu. Natomiast pozostałe konta oraz grupy wbudowane powinny być używane do wszystkich pozostałych zadań administracyjnych. Dodatkowo lokalna grupa **Administratorzy** również powinna zawierać tylko kilku wybranych użytkowników. Zarządzanie komputerem z poziomu tego konta rodzi przeróżne zagrożenia dla systemu zabezpieczeń. Przykładowo wirusy typu koło trojański mogłyby przechwycić informacje dotyczące parametrów logowania i wykorzystać je do zaatakowania systemu. Dlatego też administratorzy systemu powinni logować się do systemu jako zwykli użytkownicy. System Windows udostępnia specjalną właściwość

Uruchom jako inny użytkownik lub **Uruchom jako Administrator**, która pozwala wykonywać dowolne zadanie administracyjne w takiej sytuacji. Pozwala ona na uruchomienie programu jako dowolny inny użytkownik. Aby skorzystać z tej opcji należy:

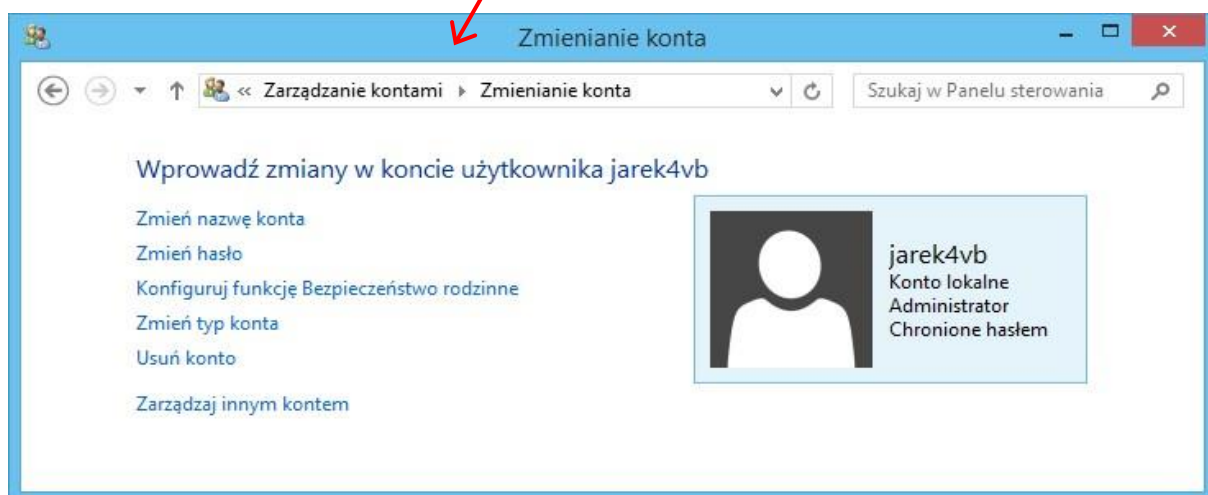
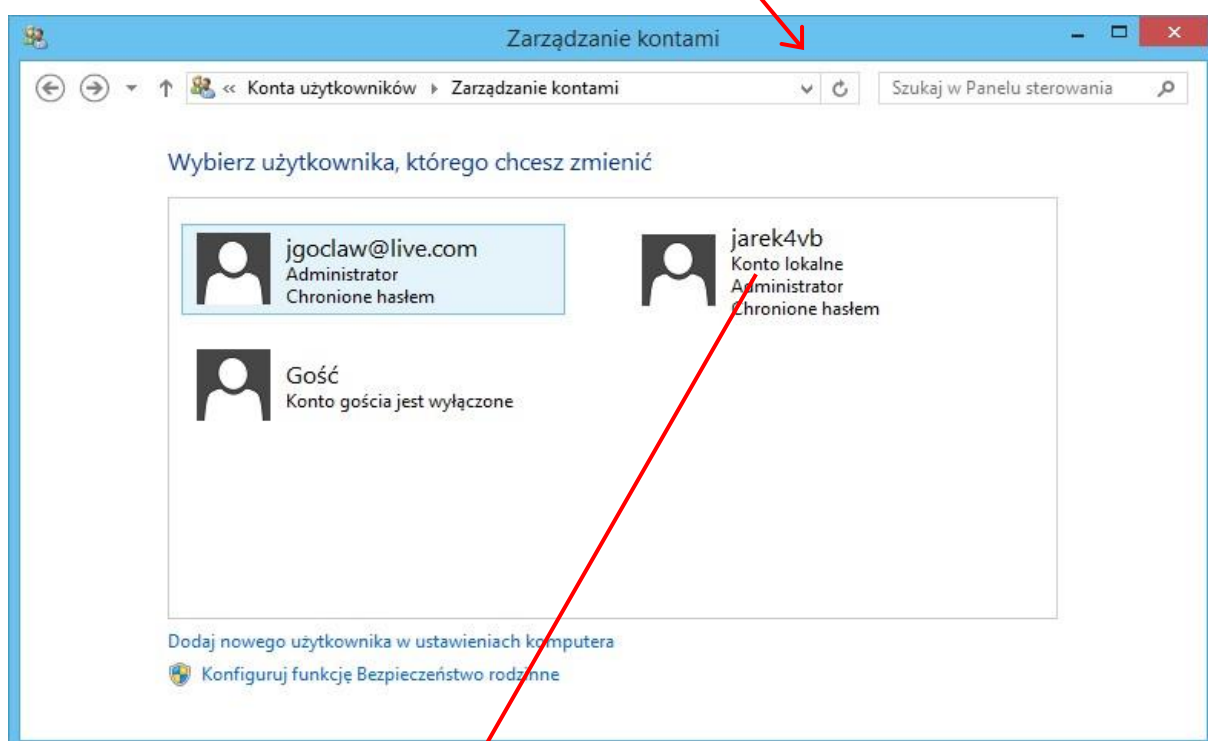
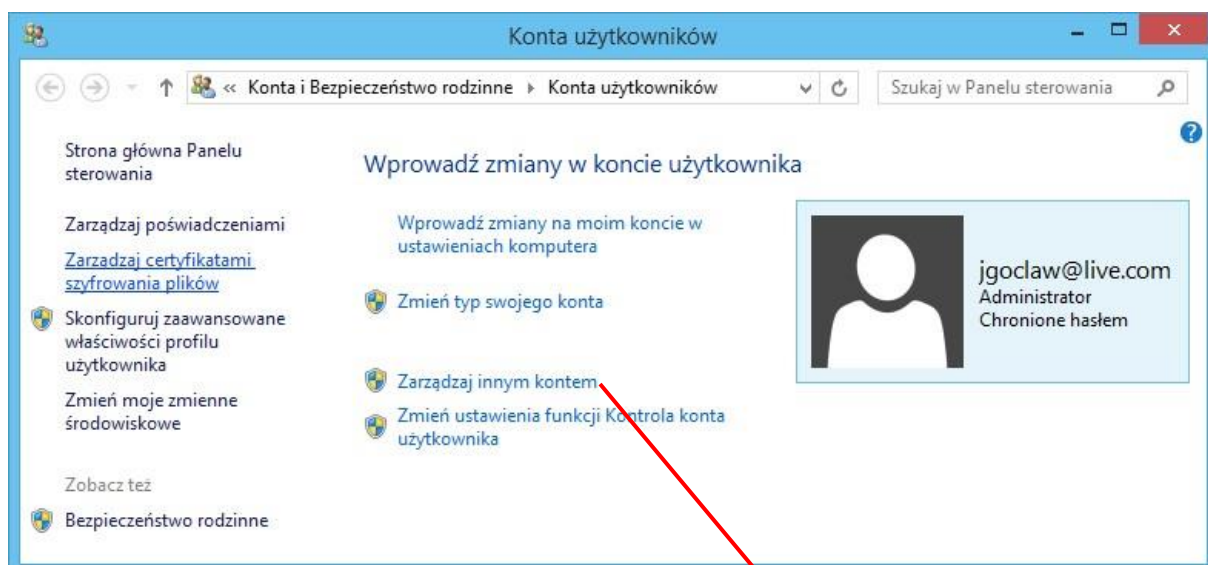
- Należy otworzyć okno programu Eksplorator Plików i wyszukać potrzebną aplikację lub plik o rozszerzeniu msc, który ma być użyty do wykonania zadania administracyjnego.
- Następnie należy przytrzymać klawisz **Shift** i kliknąć na wybranej aplikacji prawym klawiszem myszy. Z wyświetlonego menu kontekstowego należy wybrać polecenie **Uruchom jako inny użytkownik** (Rysunek).
- W wyświetlonym oknie należy wybrać, czy aplikacja ma zostać uruchomiona z bieżącego konta, czy też ma zostać uruchomiona z konta innego użytkownika.

Funkcja ta działa jako usługa. Należy się więc upewnić, czy usługa ta jest uruchomiona w konsoli **Zarządzanie komputerem** (CompMgmt.msc) (gałąź **Aplikacje i usługi** usługa **Logowanie pomocnicze**).



Ekran startowy – Konta użytkowników

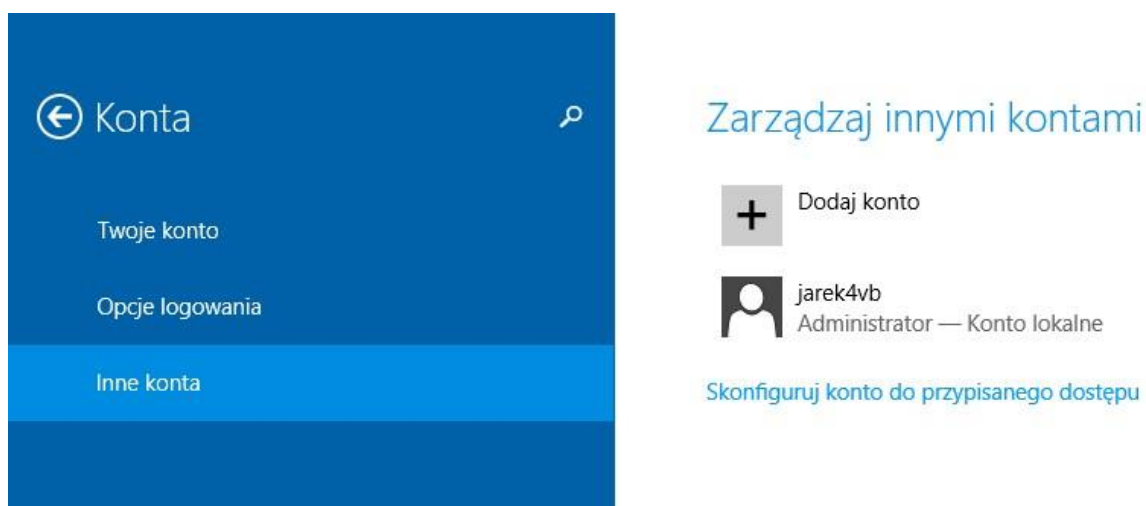
Do kont można dotrzeć poprzez **Panel Sterowania\Konta i bezpieczeństwo rodzinne\Konta użytkowników\Zarządzaj innym kontem** lub wykorzystując ikonę ustawień **Konta użytkowników** z poziomu ekranu startowego Windows („kafelki”).



Można także wpisać polecenia: Ustawienia konta, Zmień typ konta, Dodawanie i usuwanie innych kont użytkowników, Utwórz konto albo lepiej tylko słowo „konto” lub „konta” i wyszukać najbardziej odpowiednie działania z listy wybranych funkcji. Okno Zarządzanie kontami. Podwójne kliknięcie pozycji użytkownika w oknie **Zarządzanie kontami** otwiera dialog **Zmianie konta** (rys).

Ekran startowy – Ustawienia konta

Polecenia ustawień z ekranu startowego z charakterystyczną ikoną (kółko zębate) umożliwiają manipulacje kontami w nowym interfejsie Windows o rozszerzonej funkcjonalności. Należą do nich **Ustawienia konta**, **Dodawanie i usuwanie innych kont użytkowników oraz zarządzanie nimi**.

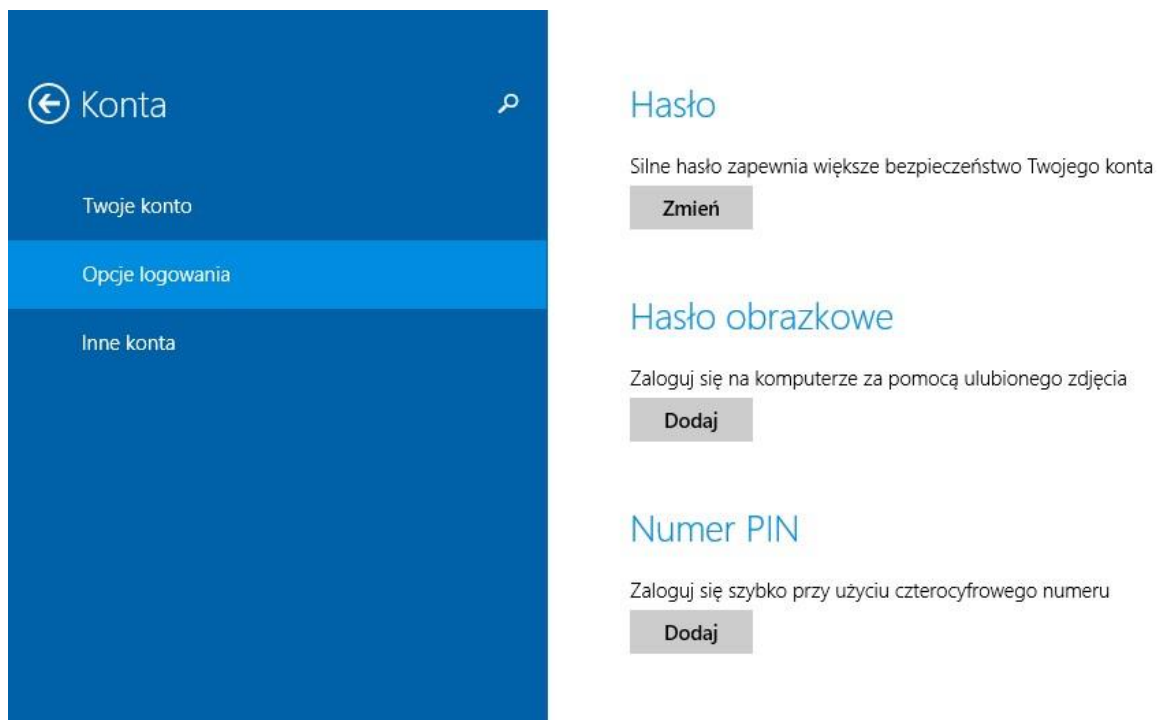


Okno otwierane poleceniem Ustawienia konta na ekranie startowym

Poprzez pozycje **Twoje konto** lub **Inne konta** można dodać usunąć, zmienić typ konta. Typy kont do wyboru:

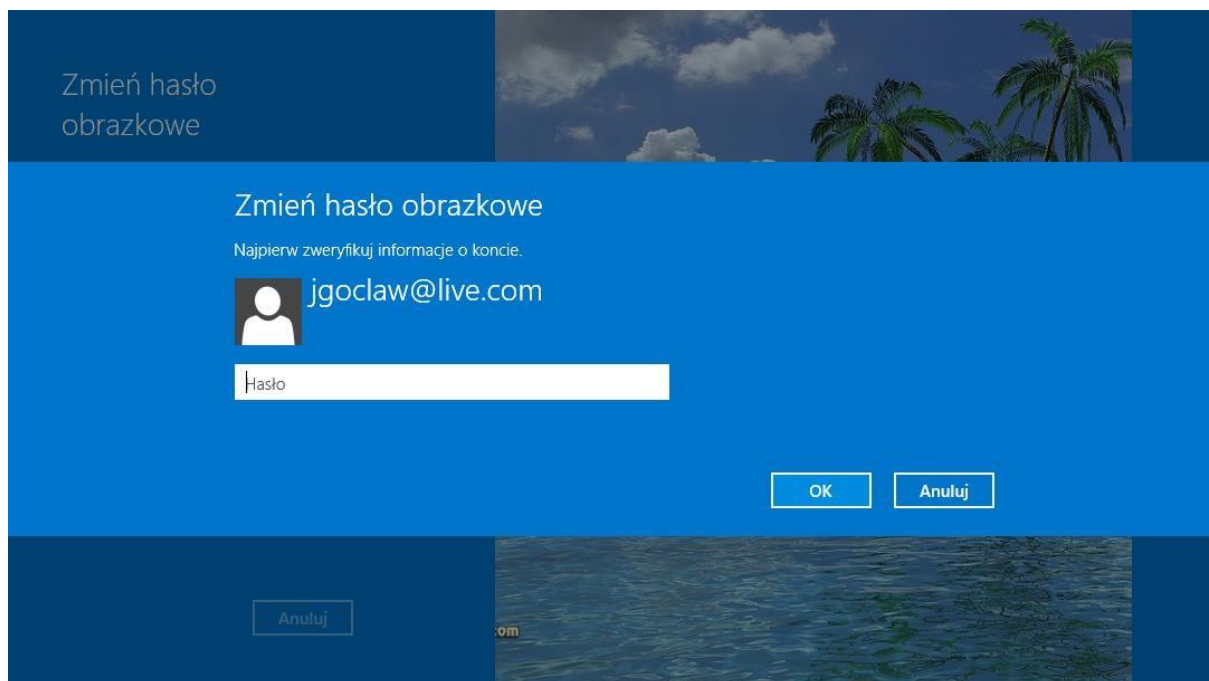
- Administrator
- Użytkownik standardowy
- Dziecko użytkownik standardowy monitorowany przez moduł Bezpieczeństwo rodzinne

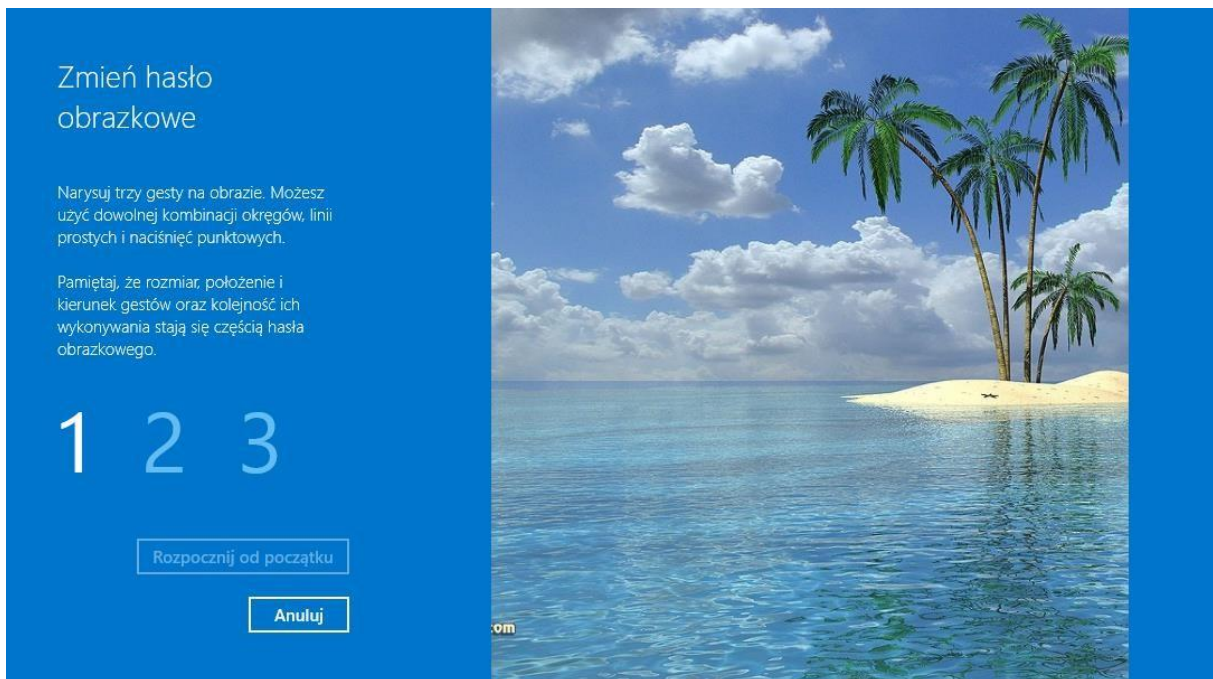
Poprzez **Ustawienia konta\Opcje logowania** można podać tradycyjne hasło do konta, uproszczone hasło w formie numeru PIN lub Hasło obrazkowe; wszystkie te opcje logowania mogą obok siebie występować dla danego konta.



Ekran opcji logowania

Hasło obrazkowe wymaga wyboru pliku obrazu przewidzianego jako tło logowania zarejestrowania dotykowo lub myszką 3 gestów na wybranym tle. Gesty powinny rysować okrąg, linię prostą lub punkt. Kolejność i kierunki zaznaczania obiektów są istotne. Gesty należy powtórzyć dwukrotnie jak w przypadku haseł.





Aplikacja NET.EXE

Program konsolowy **NET.exe**, uruchomiony w trybie Administratora może być wykorzystywany do wykonywania zadań administracyjnych związanych z kontami czy grupami użytkowników.

```
net user *nazwa_użytkownika *hasło | *+ *opcje++ */domain+  
nazwa_użytkownika ,hasło | *- /add *opcje+ */domain+  
nazwa_użytkownika */delete+ */domain+
```

Z poleceniem net user można używać następujących parametrów:

- nazwa_użytkownika
Nazwa konta użytkownika, które należy dodać, usunąć, zmodyfikować lub wyświetlić. Nazwa konta użytkownika może mieć maksymalnie 20 znaków.
- Hasło
Powoduje przypisanie lub zmianę hasła konta użytkownika. Hasło musi spełniać warunek minimalnej długości ustawiony za pomocą opcji /minpwlen polecenia net accounts. Hasło może się składać maksymalnie z 14 znaków.
- *
Powoduje wyświetlenie monitu o podanie hasła. Podczas wpisywania hasła nie jest wyświetlane.
- /domain
Powoduje wykonanie operacji na podstawowym kontrolerze domeny

- /add
Powoduje dodanie konta użytkownika do bazy danych kont użytkowników.
- /delete
Powoduje usunięcie konta użytkownika z bazy danych kont użytkowników. Opis

wszystkich opcji: <http://support.microsoft.com/kb/251394/pl>

net localgroup [<GroupName> [/comment:"<Text>"]] [/domain] **net localgroup**

[<GroupName> {/add [/comment:"<Text>"] | /delete} [/domain] **net localgroup**

*<GroupName> <Name> *...+ ,/add | /delete- */domain+

- <GroupName>
Specyfikuje nazwę grupy lokalnej przeznaczonej do utworzenia, rozszerzenia lub usunięcia. Polecenie net localgroup <GroupName> wyświetla listę użytkowników grupy lokalnej
- /comment:"<Text>"
Dodaje komentarz w apostrofach do tworzonej lub istniejącej już grupy (max 256 znaków).
- /domain
Wykonuje operację na podstawowym kontrolerze bieżącej domeny
- <Name>[...]
Listuje nazwy użytkowników i grup do dodania lub usunięcia z grupy lokalnej
- /add
Dodaje istniejącego użytkownika lub grupę globalną do podanej grupy lokalnej
- /delete
Usuwa użytkownika lub inną grupę z wskazanej grupy lokalnej.

Przykłady:

- **NET USER** Nowy Cyk4^g3B /ADD /FULLNAME:"Jan Kowalski" ⓘ utworzenie aktywnego konta użytkownika Nowy, z hasłem Cyk4^g3B i pełną nazwą.
- **NET LOCALGROUP** NowaGrupa /ADD /COMMENT:"Lokalna grupa testowa" ⓘ utworzenie nowej grupy
- **NET LOCALGROUP** NowaGrupa Nowy /ADD ⓘ dodanie użytkownika Nowy do Grupy NowaGrupa.

- **NET ACCOUNTS** ? wyświetla lokalne ustawienia kont użytkowników
- **NET USER** <login> ? wyświetla opis konta użytkownika podanego przez login

```
C:\Users\jgocl_000>net user jarek4vb
Nazwa użytkownika          jarek4vb
Pełna nazwa                 jarek4vb
Komentarz
Komentarz użytkownika
Kod kraju/regionu          000 <Domyślne ustawienia systemu>
Konto jest aktywne         Tak
Wygasanie konta            Nigdy

Hasło ostatnio ustawiano    2014-04-19 23:08:49
Ważność hasła wygasa        Nigdy
Hasło może być zmieniane    2014-04-19 23:08:49
Wymagane jest hasło         Tak
Użytkownik może zmieniać hasło Tak

Dozwolone stacje robocze    Wszystkie
Skrypt logowania
Profil użytkownika
Katalog macierzysty
Ostatnie logowanie          Nigdy

Dozwolone godziny logowania Wszystkie
Członkostwa grup lokalnych  *Administratorzy
                             *HomeUsers
                             *Użytkownicy
Członkostwa grup globalnych *Brak
Polecenie zostało wykonane pomyślnie.
```

Zadania

Konta użytkowników proszę tworzyć według następującej konwencji: Lab_d_g_n, gdzie: d - dwuliterowy skrót dnia, w którym odbywają się zajęcia laboratoryjne. g - godzina, o której zaczynają się zajęcia. n - numer kolejny konta zakładanego na laboratorium - numer ten podany jest w instrukcji.

Przykład:

Należy utworzyć konto Lab_d_g_3. Zajęciach odbywają się we wtorek o godz. 8:15 Wówczas nazwa tego konta będzie następująca: Lab_wt_8_3.

- Jakie czynności musi wykonać użytkownik, aby zalogować się do systemu?
- Jakie informacje musi dostarczyć użytkownik, aby się zalogować do systemu?
- Zaloguj się do systemu wprowadzając niewłaściwe hasło. Jaka będzie reakcja systemu na taką próbę logowania?
- Utwórz dla systemu nowe konto z logowaniem tradycyjnym (login i hasło), poprzez zarejestrowane konto Microsoft i z logowaniem przez gesty.

- Zaloguj się do systemu poprzez swoje konto Microsoft
- Zaloguj się do systemu przy pomocy loginu i hasła,
- Zaloguj się do systemu przy pomocy numeru PIN oraz gestów na wybranym obrazie tła
- Sprawdź, kto jest zalogowany na komputerze na którym aktualnie pracujesz.
- Korzystając z opcji Personalizuj\Wygaszacz ekranu wymuś, aby po włączeniu wygaszacza ekranu system był chroniony hasłem. Przetestuj to zabezpieczenie.
- Zablokuj stację roboczą i sprawdź, kto może ją odblokować?
- Jaka jest różnica między kontem domenowym i lokalnym?
- Jakie są zasady, według których powinno się tworzyć hasło dla danego konta?
- Czy można nadać tworzonemu kontu nazwę dłuższą niż 20 znaków? Utwórz takie konto i spróbuj się na nie zalogować. Sprawdź, czy w trakcie logowania można podać więcej znaków niż 20.
- Czy hasło Kowalski jest poprawne? Uzasadnij odpowiedź.
- Wykorzystując ustawienie Konta użytkowników utwórz konto o nazwie Lab_d_g_1 wpisując odpowiednie dane oraz opis. Konto powinno należeć do kategorii Użytkownik
- Zaloguj się na to utworzone w punkcie poprzednim konto. Jakie posiadasz uprawnienia?
- Zmień hasło dla użytkownika Lab_d_g_1. Czy możliwa jest zmiana hasła po zalogowaniu na to konto? Czy użytkownik sam może zmienić hasło?
- Utwórz konto o nazwie Lab_d_g_2 wykorzystując przystawkę Użytkownicy i grupy lokalne. Wymuś, aby użytkownik musiał zmienić hasło przy logowaniu i zaloguj się na to konto
- Dla konta Lab_d_g_2 włącz opcje Użytkownik nie może zmienić hasła. Sprawdź, czy elementy umożliwiające zmianę hasła są dostępne.
- Wyłącz konto Lab_d_g_2 i spróbuj zalogować się na to konto. Jaki komunikat zostanie wyświetlony?
- Utwórz przy użyciu przystawki Użytkownicy i grupy lokalne konto Lab_d_g_3 bez przypisanej grupy i sprawdź czy będzie ono widoczne w aplecie Użytkownicy i hasła. Wyjaśnij otrzymany wynik.
- Konto Lab_d_g_3 skonfiguruj tak, by miało możliwie największe restrykcje. Sprawdź ich działanie.
- Utwórz na lokalnym Lab_d_g_4. Przetestuj, na które z tych nazw można się zalogować: lab_d_g_4, Lab_d_g_4, LAB_d_g_4, lAb_d_g_4, LaB_d_g_4
- Zaloguj się na konto Lab_d_g_1 i wykorzystując polecenie Uruchom jako... wywołaj przystawkę Użytkownicy i grupy lokalne. Utwórz nowe konto Lab_d_g_5.
- Utwórz grupę Lab_d_g_lgr. Jakie pola należy obowiązkowo wypełnić przy jej zakładaniu?
- Utwórz grupę Lab_d_g_2gr. Wprowadź odpowiedni opis i dodaj do tej grupy konta Lab_d_g_1 oraz Lab_d_g_2.

- Zaloguj się na konto Lab_d_g_2. Czy zmienił się poziom uprawnień dla tego konta? Sprawdź czy możesz założyć konto Lab_d_g_6 przy użyciu ikony Ustawienia konta z ekranu startowego.
- Dodaj do grupy Lab_d_g_2gr grupę Administratorzy. Czy udało się to zrobić?
- Zaloguj się na konto Lab_d_g_2. Czy zmienił się poziom uprawnień dla tego konta? Sprawdź czy możesz założyć konto Lab_d_g_6 przy użyciu ikony Ustawienia konta z ekranu startowego
- Przypisz konto Lab_d_g_4 do grup Administratorzy i Goście. Jaki uprawnienia będzie miał ten użytkownik?
- Przypisz użytkownikowi Lab_d_g_2 folder macierzysty c:\Home\Lab_d_g_2. Jakie kroki musisz wykonać? Czy po zalogowaniu zaobserwujesz jakieś zmiany w funkcjonowaniu tego konta?

Uprawnienia

Mechanizm uprawnień w Windows

Bardzo ważną kwestią w przypadku administracji systemem Windows jest właściwe zabezpieczenie zasobów przed nieautoryzowanym dostępem. Mechanizmem zapewniającym takie zabezpieczenia są uprawnienia NTFS. Pozwalają one określić, którzy użytkownicy lub grupy mają dostęp do danego folderu lub pliku. Oczywiście w ten sposób można zabezpieczać zarówno całe foldery, jak i pojedyncze pliki.

Uprawnienia NTFS są dostępne wyłącznie na dyskach z systemem NTFS, nie są dostępne natomiast na partycjach sformatowanych z użyciem systemu plików FAT32. Uprawnienia do folderów

Uprawnienia do folderów pozwalają na kontrolę dostępu do folderów oraz do znajdujących się w nich plików i podfolderów. Poniższa tabela zawiera listę standardowych uprawnień do folderów wraz z ich opisem.

Standardowe prawa dostępu do folderów

Uprawnienia do folderów pozwalają na kontrolę dostępu do folderów oraz do znajdujących się w nich plików i podfolderów. Poniższa tabela zawiera listę standardowych uprawnień do folderów wraz z ich opisem.

Odczyt	przeglądanie zawartości katalogów oraz odczyt atrybutów i uprawnień
--------	---

Wyświetlanie zawartości folderu	Odczyt + możliwość przechodzenia przez folder, nawet gdy użytkownik nie ma uprawnień do folderów, przez które chce przechodzić
Odczyt i wykonanie	Odczyt + przechodzenie przez folder
Zapis	tworzenie nowych plików i podfolderów w danym folderze oraz zmiana atrybutów folderu
Modyfikacja	Zapis + Odczyt i wykonanie + możliwość usuwania danego folderu
Pełna kontrola	Modyfikacja + zmiany uprawnień do folderu oraz przejęcie go na własność

Uprawnienia do plików

Uprawnienia do plików pozwalają kontrolować dostęp do plików. Tabela zawiera listę standardowych uprawnień do plików z opisem.

Standardowe prawa dostępu do plików

Odczyt	Odczyt zawartości plików, podgląd jego atrybutów oraz uprawnień
Odczyt i wykonanie	Odczyt + możliwość uruchomienia pliku
Zapis	zapis oraz dołączanie danych do pliku, zmiana jego atrybutów
Modyfikacja	Zapis + odczyt i wykonanie + możliwość usuwania danego pliku
Pełna kontrola	Modyfikacja + możliwość zmiany uprawnień do pliku oraz przejęcia go na własność

W przypadku partycji sformatowanych z użyciem NTFS domyślnie do głównego katalogu przypisywane jest uprawnienie Pełna kontrola dla grupy Wszyscy. Grupa Wszyscy ma więc dostęp do wszystkich folderów oraz plików, tworzonych w katalogu głównym. Aby dostęp do plików i folderów mieli tylko autoryzowani użytkownicy, należy zmienić domyślne uprawnienia do tworzonych plików i folderów.

Lista kontroli dostępu

System plików NTFS wraz z każdym plikiem i folderem przechowuje na dysku listę kontroli dostępu (ACL – Access Control List). Lista ta zawiera spis wszystkich kont użytkowników i grup, które mają nadany dostęp do plików i folderów oraz typ dostępu, jaki został im nadany. Aby użytkownik mógł skorzystać z danego pliku lub folderu, na liście ACL musi istnieć wpis zwany Access Control Entry (ACE) dla niego lub grupy, do której on należy. Wpis ten musi pozwalać na rodzaj dostępu, który jest nadany (np. odczyt) dla użytkownika, który chce ten dostęp

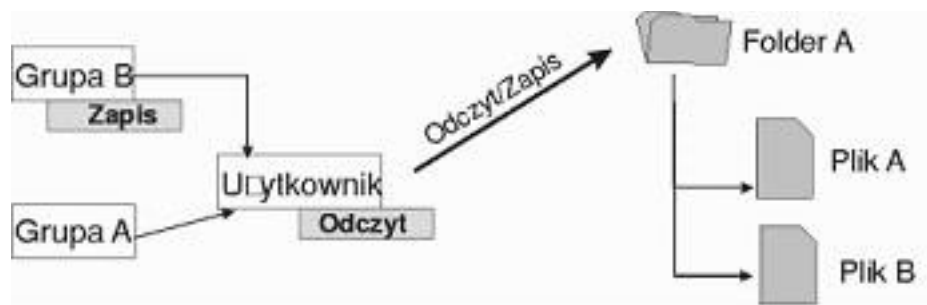
uzyskać. Jeśli wpis ACE nie występuje na liście ACL, wówczas użytkownik nie będzie miał dostępu do danego zasobu.

Uprawnienia wielokrotne

Poprzez przypisanie różnych uprawnień dla użytkownika i dla grupy, do której on należy może się zdarzyć, iż będzie on miał przypisane różne uprawnienia do danego zasobu. Aby poprawnie przypisywać uprawnienia, należy zrozumieć sposoby nakładania się i dziedziczenia uprawnień dla systemu NTFS.

Kumulowanie uprawnień

Efektywne uprawnienia dla użytkownika są kombinacją uprawnień przypisanych dla niego samego oraz dla grupy, do której on należy. Jeśli użytkownik posiada prawo do odczytu danego folderu (uprawnienie Odczyt), a grupa, której jest członkiem posiada prawo na zapis (uprawnienie Zapis), wówczas użytkownik ma oba rodzaje uprawnień do tego katalogu (Odczyt oraz Zapis). Następuje więc kumulacja uprawnień dla użytkownika i dla grupy, do której on należy. Sytuację tę przedstawia poniższy rysunek.



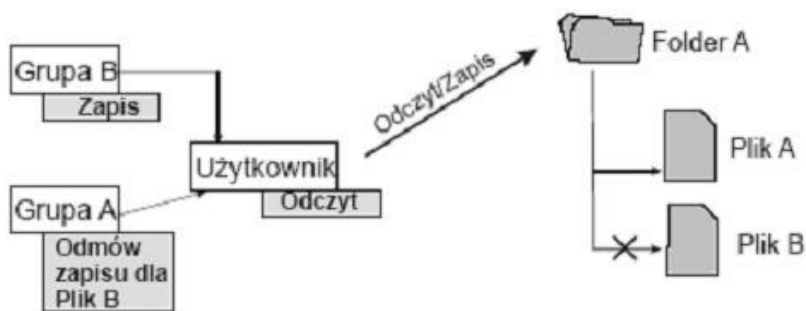
Kumulowanie uprawnień

Nadpisywanie uprawnień

Uprawnienia do plików w systemie NTFS mają wyższy priorytet niż uprawnienia do folderów. Oznacza to, że jeśli użytkownik będzie miał odpowiednie uprawnienia do pliku, to będzie miał do niego dostęp, nawet jeśli nie będzie miał dostępu do folderu, w którym ten plik się znajduje. Aby skorzystać z tego pliku, użytkownik musi podać pełną ścieżkę dostępu zgodną z konwencją UNC (Universal Naming Convention) lub też lokalną ścieżkę dostępu.

Uprawnienie Odmawiaj

W systemie Windows istnieje możliwość zabronienia użytkownikowi lub grupie dostępu do wybranego pliku lub folderu. Aby to zrobić należy przypisać danemu zasobowi uprawnienie Odmawiaj. Nie jest to jednak zalecany sposób kontroli dostępu do zasobów. Uprawnienie to spowoduje zablokowanie wszystkich innych uprawnień, mimo iż użytkownik może mieć zdefiniowane uprawnienia, które pozwolą mu na dostęp do tego zasobu. Przykład zaprezentowany na rysunku wyjaśnia tę sytuację.



Działanie uprawnienia Odmawiaj

Użytkownik1 ma prawo Odczyt dla Folder_A i jest członkiem grupy Grupa1 oraz Grupa2. Grupa2 ma prawo Zapis do folderu Folder_A. Równocześnie grupa Grupa1 ma zabronione prawo Zapis dla pliku Plik2. Użytkownik może czytać i zapisywać plik Plik1. Ponadto może odczytywać plik Plik2, ale nie może zapisywać tego pliku, ponieważ jest członkiem grupy Grupa1, która ma zablokowane prawo Zapis dla pliku Plik2. Uprawnienie Odmawiaj jest jedynym wyjątkiem od zasady kumulowania uprawnień. Dlatego tego sposobu kontroli dostępu do zasobów należy unikać. Znacznie prostszym sposobem kontroli dostępu jest zezwalanie na dostęp do odpowiednich zasobów tylko wybranym użytkownikom i grupom. Należy więc tak projektować grupy oraz organizować drzewo folderów, aby zarządzanie zasobami i dostępem do nich odbywało się poprzez zezwalanie na dostęp, bez potrzeby korzystania z uprawnienia Odmawiaj.

Dziedziczenie uprawnień

Domyślnie uprawnienia, które przypisywane są do folderów nadrzędnych są dziedziczone przez podfoldery i pliki w nim zawarte. Przypisanie uprawnień do danego folderu spowoduje przypisanie takich samych uprawnień do wszystkich w nim istniejących, jak i nowo tworzonych, plików i folderów. Istnieje jednak możliwość zablokowanie dziedziczenia uprawnień. Zablokowanie dziedziczenia uprawnień spowoduje, że wyłączone zostanie przekazywanie uprawnień z folderu macierzystego do podfolderów i plików w nim zawartych. Aby wyłączyć ten mechanizm należy w podfolderach i plikach usunąć wszystkie odziedziczone uprawnienia, pozostawiając pozostałe uprawnienia. Folder, dla którego zablokowano mechanizm dziedziczenia uprawnień staje się teraz nowym folderem nadrzędnym i jego uprawnienia będą teraz dziedziczyły jego podfoldery i pliki.

Przypisywanie i modyfikowanie uprawnień

Narzędzie edycji uprawnień

Użytkownicy z grupy Administratorzy lub z prawem Pełna kontrola oraz właściciele plików i folderów mogą przypisywać uprawnienia dla grup i użytkowników. W tym celu należy kliknąć na wybranym pliku lub folderze i wybrać polecenie **Właściwości**, a następnie wybrać zakładkę **Zabezpieczenia**. Wygląd zakładki **Zabezpieczenia** został przedstawiony na rysunku.

Na zakładce tej dostępne są następujące opcje:

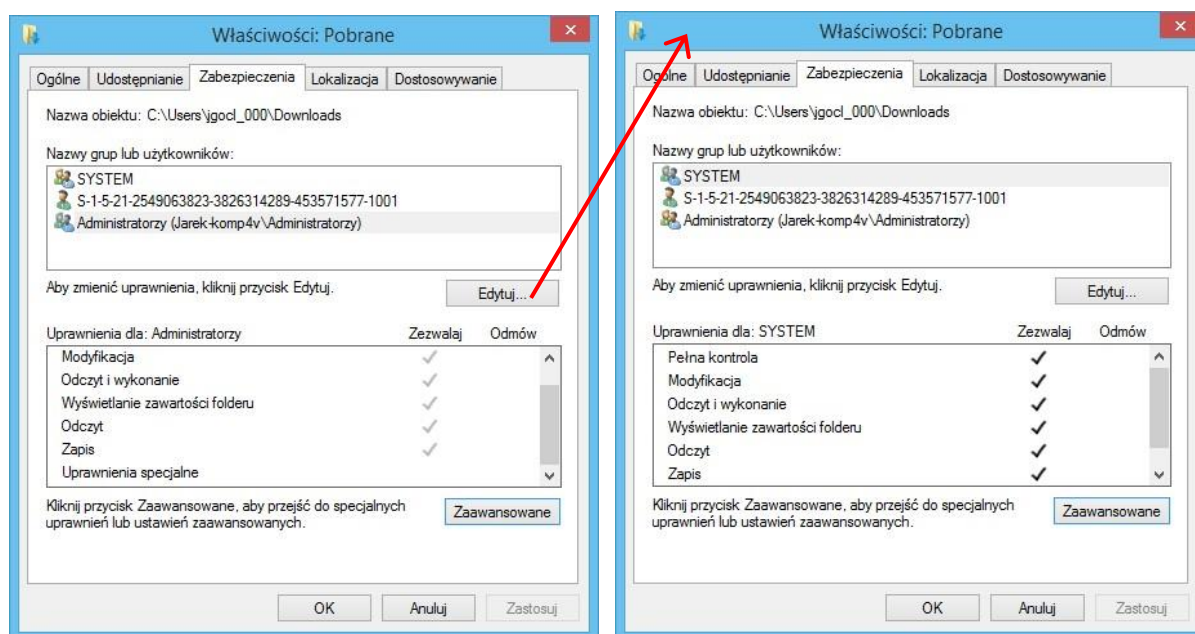
Nazwy grup lub użytkowników pole to zawiera listę grup lub użytkowników, którzy mają przypisane uprawnienia do danego zasobu.

Uprawnienia dla:

lista wszystkich praw wybranych użytkowników, które można ustawić dla danego zasobu.

Edytuj otwiera okno **Uprawnienia** z przyciskami dodawania, usuwania użytkowników i grup uprawnionych do posługiwania się wskazanym zasobem oraz polami wyboru podstawowych uprawnień

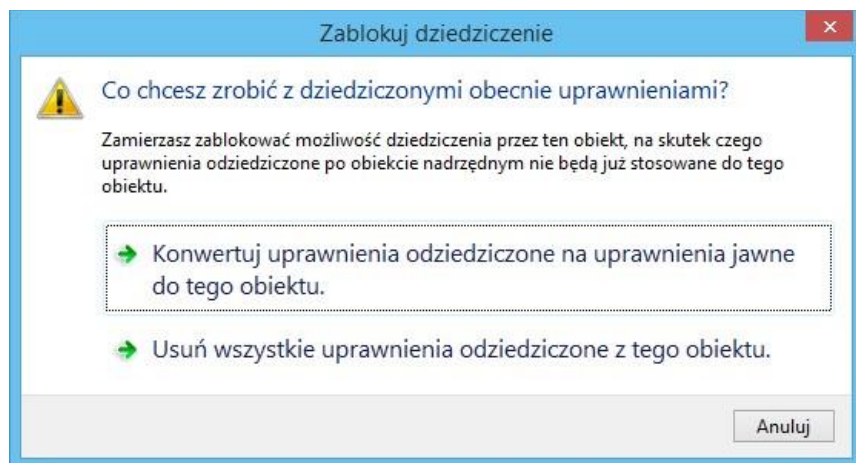
Zaawansowane przycisk ten otwiera okno **Zaawansowane ustawienia zabezpieczeń**, w którym można ustawiać dodatkowe uprawnienia do danego zasobu po uprzednim wyłączeniu ich dziedziczenia.



Jeżeli pole wyboru uprawnienia jest wyszarzone, oznacza to, że dane uprawnienie zostało odziedziczone z folderu nadrzędnego. Dziedziczenie uprawnień wyłącza się w oknie pod przyciskiem **Zaawansowane**.

Wyłączanie dziedziczenia uprawnień

Domyślnie podfoldery oraz pliki dziedziczą uprawnienia, które są przypisane do ich folderu nadrzędnego. Przycisk **Wyłącz dziedziczenie** w oknie ustawień zaawansowanych (rysunek kolejny) wyłącza dziedziczenie uprawnień. Zostanie wówczas wyświetlony dialog **przedstawiony na rysunku**.



Opcje dostępne w tym oknie to: **Konwertuj...**

opcja ta pozwala na skopiowanie uprawnień z folderu nadrzędnego do bieżącego folderu, a następnie blokuje dziedziczenie uprawnień z folderu nadrzędnego. **Usuń...**

opcja ta powoduje, że uprawnienia które są odziedziczone z folderu nadrzędnego zostają usunięte z podfolderów i plików, a pozostają tylko uprawnienia przypisane bezpośrednio do plików lub podfolderów. **Anuluj** przycisk ten powoduje anulowanie wprowadzanych zmian.

Uprawnienia specjalne

Standardowe uprawnienia NTFS dają użytkownikom systemu Windows wystarczające sposoby do kontroli i zabezpieczania dostępu do zasobów. Może jedna wystąpić sytuacja, kiedy administrator systemu nie będzie w stanie określić poziomu dostępu do zasobów, jakiego wymagają użytkownicy. W takim przypadku należy skorzystać ze specjalnych uprawnień systemu NTFS. W systemie Windows dostępnych jest 13 takich uprawnień. Uprawnienia standardowe są kombinacją uprawnień specjalnych. Przykładowo, uprawnienie standardowe Odczyt jest kombinacją uprawnień specjalnych: Odczyt danych, Odczyt uprawnień, Odczyt atrybutów oraz Odczyt rozszerzonych atrybutów. Jeżeli przypisujemy specjalne uprawnienia do folderu, możemy wybrać czy uprawnienia będą odziedziczone przez podfoldery i pliki znajdujące się w tym folderze.

TABELA

Uprawnienia specjalne	Pełna kontrola	Modyfikacja	Zapis	Wyświetlanie zaw. folderu	Odczyt i wykonanie	Odczyt
Przechodzenie przez folder/Wykonywanie pliku	X	X		X	X	

Wyświetlanie zawartości folderu/ Odczyt danych	X	X		X	X	X
Odczyt atrybutów	X	X		X	X	X
Odczyt atrybutów rozszerzonych	X	X		X	X	X
Tworzenie Plików/Zapis danych	X	X	X			
Tworzenie folderów/ Dołączanie danych	X	X	X			
Zapis atrybutów	X	X	X			
Zapis atrybutów rozszerzonych	X	X	X			
Usuwanie podfolderów i plików	X					
Usuwanie	X	X				
Odczyt uprawnień	X	X		X	X	
Zmiana uprawnień	X					
Przejęcie na własność	X					

Uprawnienie Zmiana uprawnień

Uprawnienie to pozwala administratorowi lub użytkownikowi na przypisanie lub zmianę uprawnień dla danego pliku lub folderu, bez przypisanego uprawnienia Pełny dostęp. W ten sposób, użytkownik lub administrator nie może skasować lub zapisać pliku lub folderu, ale będzie mógł przypisać uprawnienia do pliku lub folderu. Aby administratorzy systemu mogli zmieniać uprawnienia dla danego zasobu, należy grupie Administratorzy przypisać uprawnienie Zmiana uprawnień.

Uprawnienie Przejęcie na własność

Uprawnienie to pozwala innemu użytkownikowi, grupie lub Administratorowi na przejęcie na własność pliku lub folderu. Przy przejmowaniu zasobu na własność obowiązują następujące zasady:

Użytkownik z prawem Pełny dostęp może przypisać prawo Pełny dostęp lub Przejęcie na własność innemu użytkownikowi lub grupie. Pozwoli to użytkownikowi lub członkowi tej grupy na przejęcie danego pliku lub folderu na własność.

Właściciel pliku lub folderu zawsze może kontrolować i modyfikować uprawnienia swoich plików i folderów, nawet jeśli nie ma jawnie przypisanego prawa Pełny dostęp lub Zmiana uprawnień (uprawnienie zaawansowane).

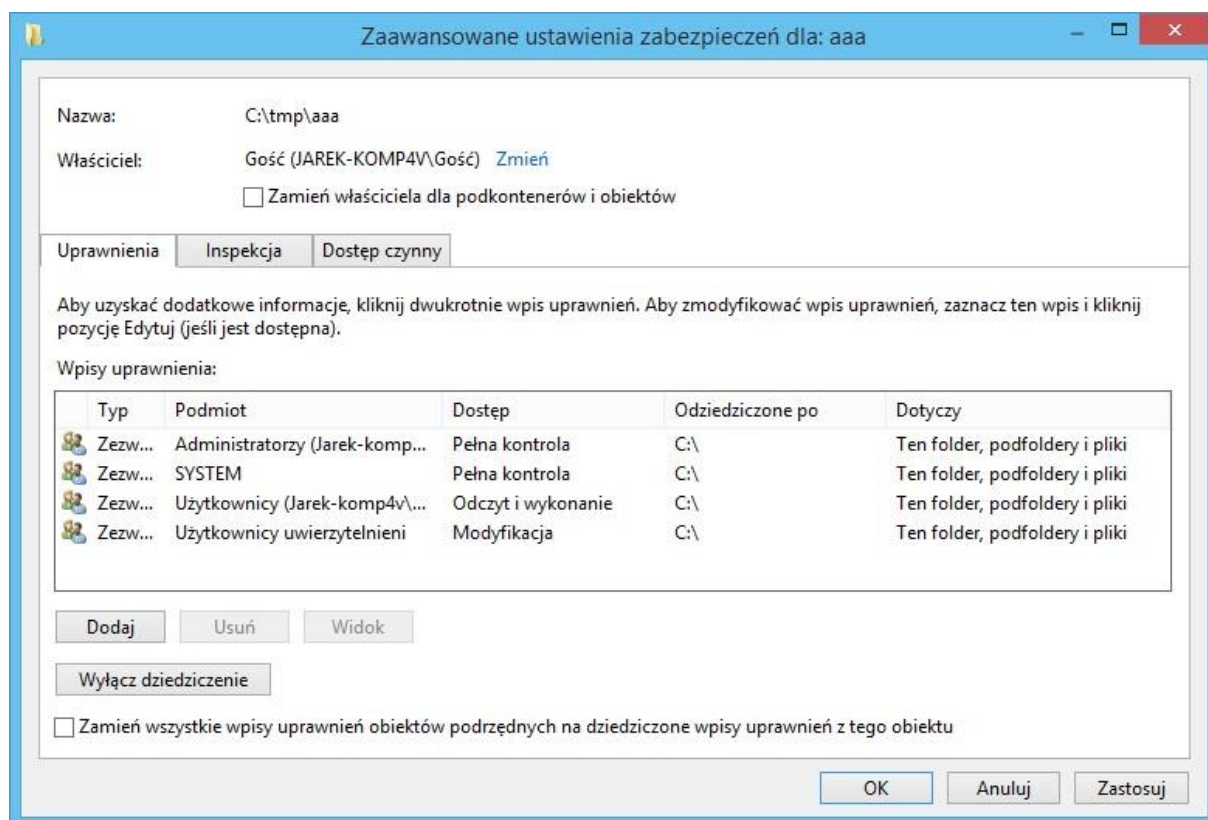
Administrator może przejść na własność folder lub plik bez względu na przypisane do niego uprawnienia. Jeśli administrator przejmie folder lub plik na własność, właścicielem pliku staje się grupa Administratorzy. Każdy członek tej grupy może zmienić uprawnienia dla pliku lub folderu oraz przypisać uprawnienie Przejęcie na własność innemu użytkownikowi lub grupie.

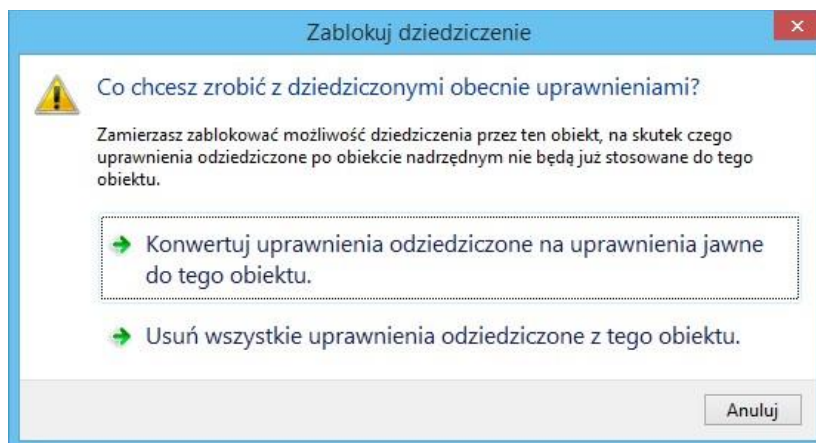
Aby stać się właścicielem danego pliku lub folderu należy skorzystać z uprawnienia Przejęcie na własność. Nie możemy zdecydować, że inny użytkownik stanie się właścicielem danego zasobu. Aby stać się właścicielem danego zasobu, użytkownik lub grupa z uprawnieniem Przejęcie na własność musi w sposób jawny przejść na własność dany zasób.

Przypisywanie specjalnych uprawnień

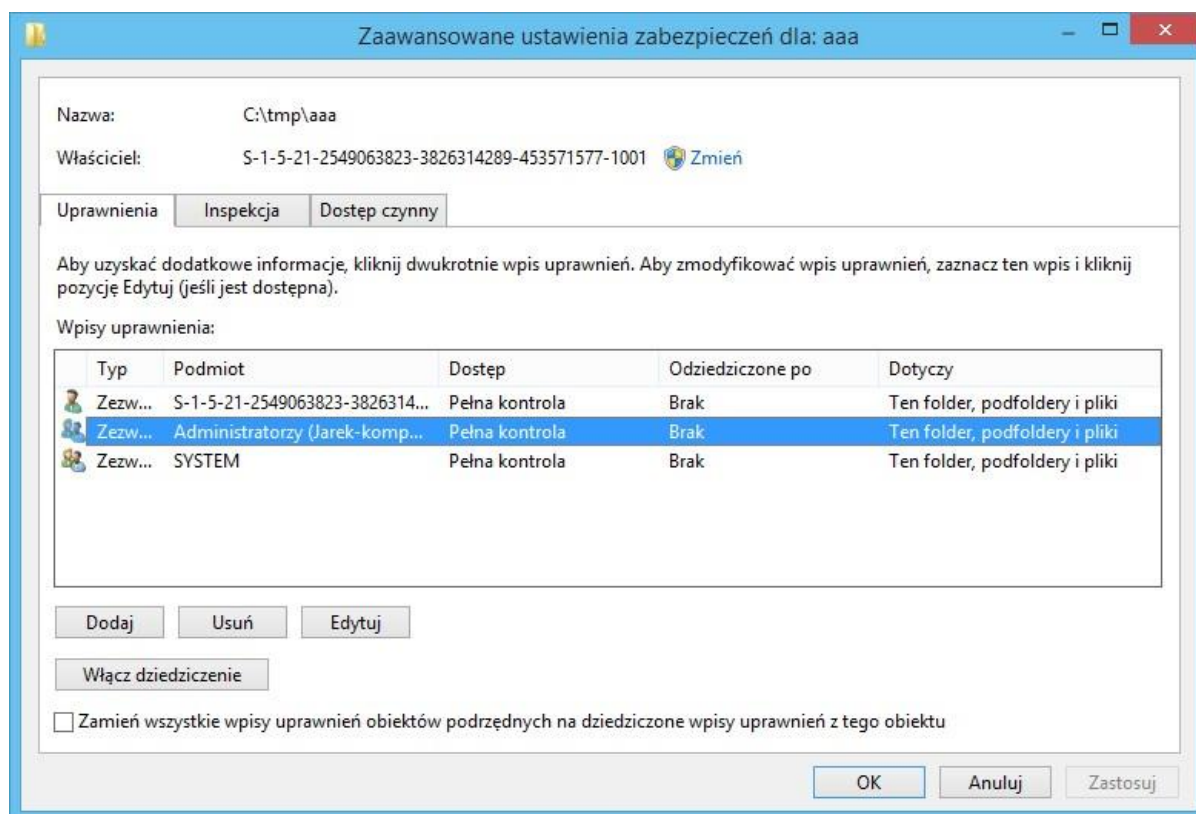
Aby przypisać użytkownikowi lub grupie specjalne uprawnienia należy:

- W oknie dialogowym **Właściwości** danego pliku lub folderu na zakładce **Zabezpieczenia** wybrać przycisk **Zaawansowane**.
- W oknie dialogowym **Zaawansowane ustawienia zabezpieczeń** (rys.) na zakładce **Uprawnienia** należy wskazać użytkownika lub grupę, dla której chcemy ustawić lub zmodyfikować uprawnienia specjalne i po wyłączeniu dziedziczenia uprawnień (typowo włączone) nacisnąć przycisk **Edytuj**.

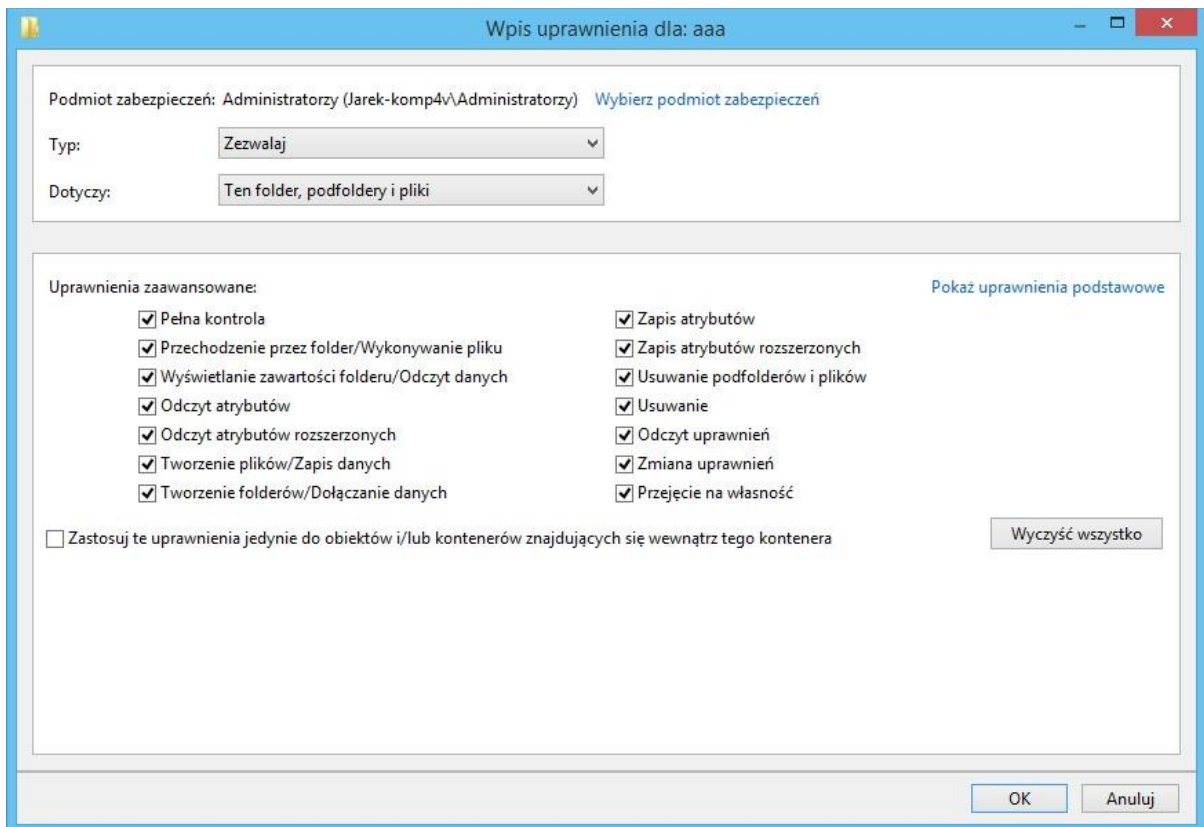




- W oknie dialogowym **Wpis uprawnienia** należy włączyć uprawnienia zaawansowane i skonfigurować odpowiednio opcje.



Zaawansowane ustawienia zabezpieczeń po wyłączeniu dziedziczenia.

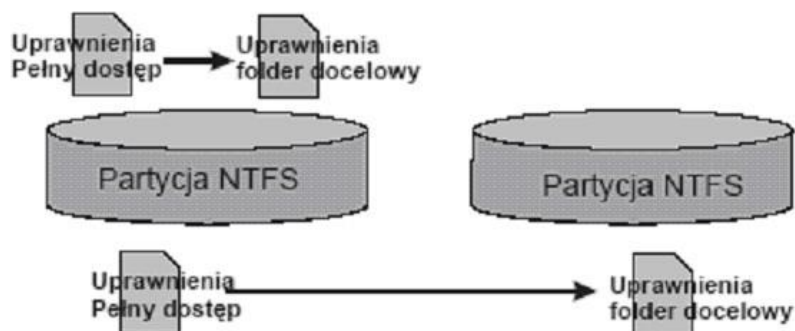


Kopiowanie i przenoszenie plików i folderów

W czasie kopiowanie lub przenoszenia plików i folderów, uprawnienia dla nich ustawione mogą się zmienić. Zmiana tych uprawnień jest ściśle określona i zależy od tego, gdzie i w jaki sposób dany został umieszczony.

Kopiowanie zasobów

Podczas kopiowania plików lub folderów do innego folderu zarówno w obrębie tej samej partycji, lub też innej partycji NTFS - uprawnienia kopii dziedziczą uprawnienia folderu docelowego. Sytuacja ta została przedstawiona na rysunku.



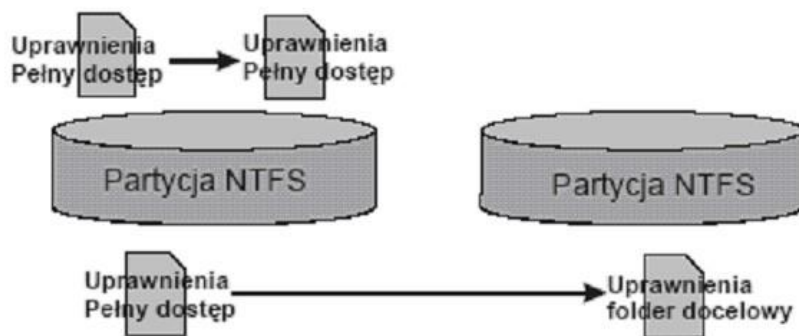
Warto więc zapamiętać:

- Windows traktuje kopiowany plik lub folder jako zupełnie nowy zasób. Jako nowy zasób przejmuje więc on swoje uprawnienia od folderu docelowego.

- Aby móc skopiować plik do folderu docelowego, Użytkownik musi posiadać prawo Zapis.
- Użytkownik, który kopiuje plik staje się jego Twórca Właścicielem.
- Podczas kopiowanie danych na partycję opartą na systemie plików FAT32 tracimy wszystkie uprawnienia, jakie były do nich przypisane.

Przenoszenie zasobów

Podczas przenoszenia zasobów, uprawnienia do nich mogą się zmienić lub nie. Zależy to od tego, gdzie przenoszony jest dany zasób (Rysunek).



Jeśli dane (pliki i/lub foldery) przenoszone są w obrębie tej samej partycji NTFS, wówczas:

- Zachowują swoje oryginalne uprawnienia.
- Aby móc je przenieść, użytkownik musi posiadać prawo Zapis do folderu docelowego.
- Użytkownik musi posiadać prawo Modyfikacja do folderu źródłowego, ponieważ przenoszone dane muszą zostać z tego folderu usunięte.
- Właściciel danych nie zmienia się.
- Jeśli dane (pliki i/lub foldery) przenoszone są na inną partycję NTFS, wówczas:
- Dziedziczą uprawnienia od folderu docelowego.
- Aby móc je przenieść, użytkownik musi posiadać prawo Zapis do folderu docelowego.
- Użytkownik musi posiadać prawo Modyfikacja do folderu źródłowego, ponieważ przenoszone dane muszą zostać z tego folderu usunięte.
- Użytkownik, który przenosi te dane staje się Twórca Właścicielem.

Podczas przenoszenia danych na partycje oparte o system plików FAT16 i FAT32 tracimy wszystkie uprawnienia, jakie były do tych danych przypisane.

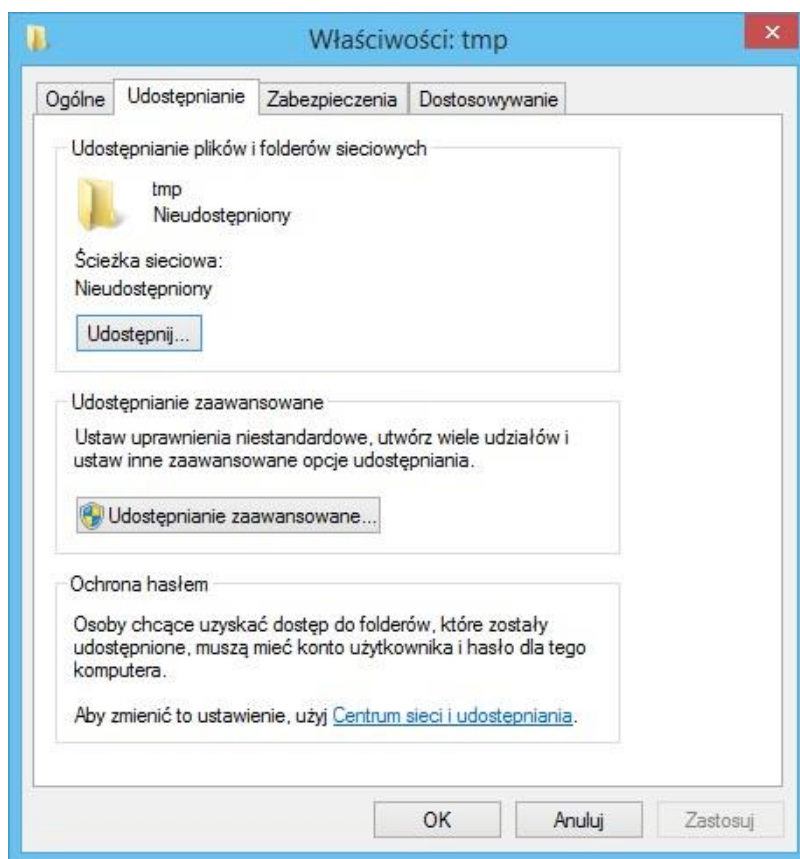
Zadania

- Jako admin utworzyć na dysku C:\ folder o nazwie Folder_d_g i utworzyć tam pięć dowolnych plików tekstowych o nazwach podobnych do plik1.txt
- Przypisać do niego następujące prawa dostępu (należy wyłączyć dziedziczenie od folderu nadrzędnego):
 - dla Lab_d_g_11gr prawo Pełnej Kontroli
 - dla Lab_d_g_12gr prawo tylko do odczytu, wykonywania i wyświetlania zawartości.
 - dla Lab_d_g_12gr w uprawnieniach specjalnych dołożyć uprawnienie do usuwania plików i podfolderów
 - dla grupy Administratorzy ustawić uprawnienia Pełnej Kontroli
- Czy użytkownik Lab_d_g_12 może modyfikować plik plik1.txt? W tym celu zaloguj się jako użytkownik Lab_d_g_12.
- Użytkownik Lab_d_g_11 należy do obu grup i raz ma Pełną Kontrolę a raz tylko odczyt. Czy może modyfikować plik plik1.txt?
- Dla Lab_d_g_12gr ustanowić prawo „Odmawiaj usuwania”. Sprawdź, który z użytkowników może usunąć dowolny plik.
- Odznaczyć prawo „Odmawiaj usuwania” dla grupy Lab_d_g_12gr.
- Znajdź plik **compmgmt.msc**. Uruchom go będąc zalogowany jako użytkownik Lab_d_g_11. Czy możesz zapisać dowolny dokument w katalogu systemowym? Zamknij program i następnie otwórz go korzystając z polecenia Uruchom jako... i sprawdź, czy teraz możesz wykonać wcześniejszą operację.
- Jako admin utworzyć dwie grupy lokalne o nazwach: Lab_d_g_11gr i Lab_d_g_12gr (notacja zgodna z ćwiczeniem dt. kont użytkowników)
- Utworzyć dwóch użytkowników lokalnych o nazwach: Lab_d_g_11 i Lab_d_g_12
- Użytkownika Lab_d_g_11 o przydzielić do grup: Lab_d_g_11gr i Lab_d_g_12gr o nadać hasło takie, jak nazwa użytkownika
- Użytkownika Lab_d_g_12 o przydzielić tylko do grupy: Lab_d_g_12gr o wymusić, aby użytkownik musiał zmienić hasło przy logowaniu o nadać hasło w postaci „abc123”
- Jako użytkownik admin przenieś folder Folder_d_g do katalogu c:\Work. Sprawdź, co się stało z uprawnieniami nowego obiektu.
- Jako użytkownik admin skopiuj folder Folder_d_g na dysk c:\. Sprawdź, co się stało z uprawnieniami nowego obiektu.
- Jako użytkownik admin skopiuj folder c:\Work\Folder_d_g na dysk d:\. Sprawdź, co się stało z uprawnieniami nowego obiektu.
- Jako użytkownik admin przenieś folder c:\Work\Folder_d_g na dysk d:\. Sprawdź, co się stało z uprawnieniami nowego obiektu.

Udostępnianie plików i folderów

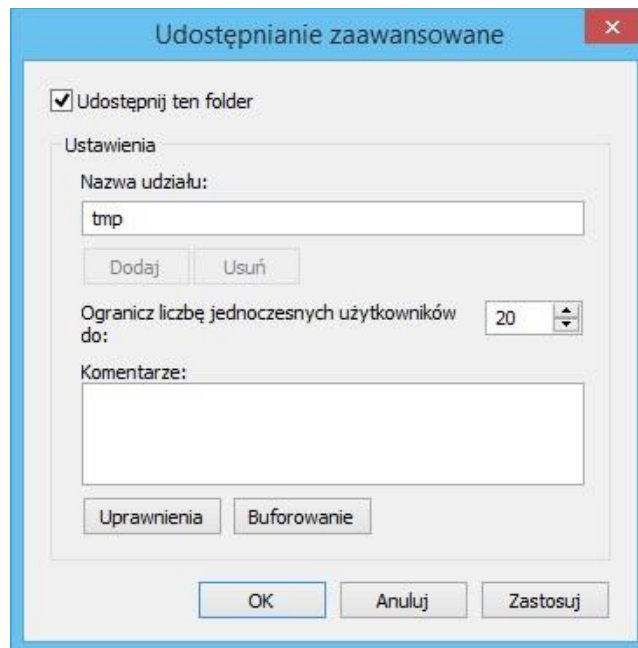
Tworzenie udziału

Aby dodać nowy udział należy ustawić się na wymaganej pozycji w Eksploratorze Plików i po kliknięciu prawym przyciskiem myszki wybrać z menu rozwijalnego opcję **Właściwości**, a następnie zakładkę **Udostępnianie**. Zakładka ta umożliwia udostępnianie udziałów, zmianę uprawnień do nich oraz ustawienie buforowania dla programów i plików. W zakładce można wykonać udostępnianie proste plików i folderów sieciowych (przycisk **Udostępnianie...**) lub udostępnianie zaawansowane przy posiadaniu uprawnień administracyjnych (przycisk **Udostępnianie zaawansowane...**).

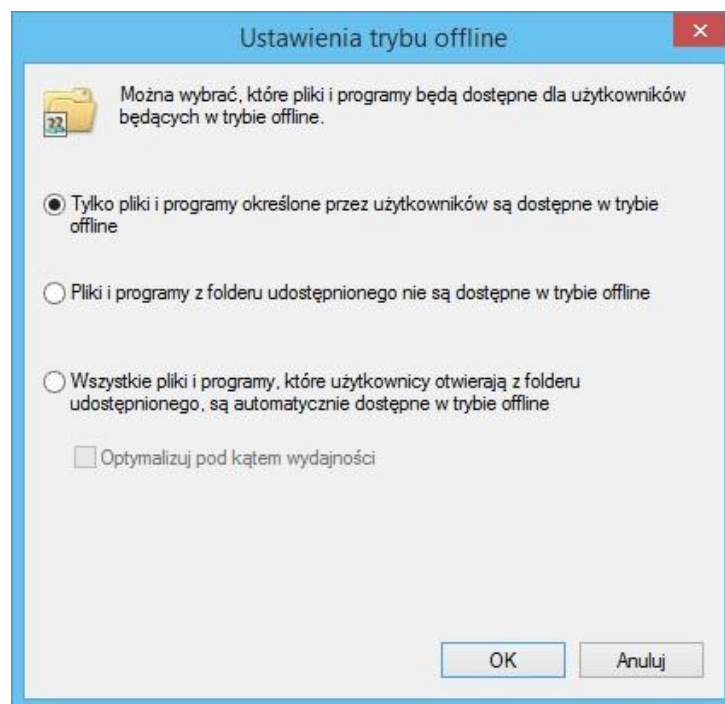


W oknie **Udostępnianie zaawansowane** można ustawić:

- Nazwę udziału,
- Liczbę jednoczesnych użytkowników,
- Uprawnienia dla udziału (Odczyt, Zmiana, Pełna kontrola) ☐ Buforowanie.



Aby dostosować opcje buforowania należy kliknąć przycisk **Buforowanie**.

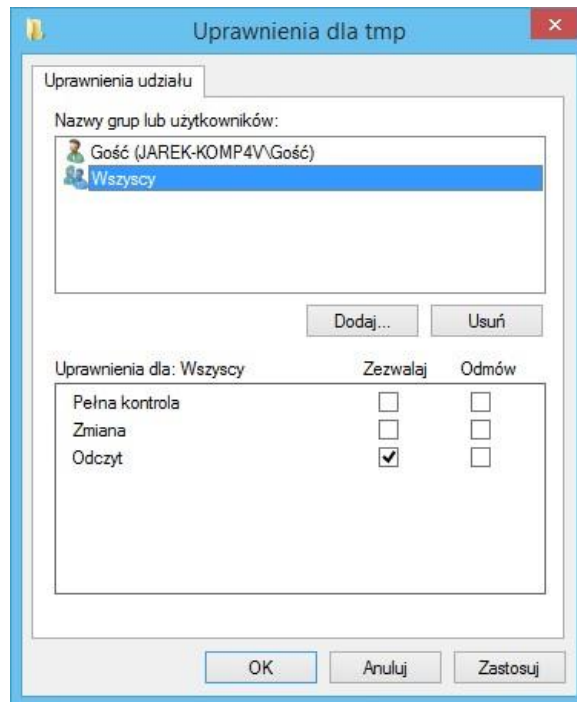


Opcje buforowania udziałów

W wyświetlonym oknie dialogowym będzie możliwe dostosowanie opcji buforowania, co pozwoli określić czy i w jaki sposób pliki będą lokalnie buforowane, gdy używają ich inni użytkownicy. Do wyboru są trzy możliwości pokazane w oknie dialogowym **Ustawienia trybu offline**.

Aby nadać grupie użytkowników szczegółowe uprawnienia do udostępnianego zasobu używany jest przycisk **Uprawnienia** w oknie **Udostępnianie zaawansowane**. W wyświetlonym oknie dialogowym **Uprawnienia dla** będzie można sprawdzić, kto ma uprawnienie do danego

udziału. Aby dodać nową grupę użytkowników należy kliknąć przycisk **Dodaj**. Spowoduje to wyświetlenie następnego okna dialogowego Wybieranie: Użytkownicy, Komputery lub Grupy. W oknie tym będzie można wybrać użytkowników, grupy lub komputery, które będą miały dostęp do danego zasobu.



Innym sposobem prostego udostępnienia folderu jest kliknięcie na nim prawym klawiszem myszy w Eksploratorze Plików i wybór opcji **Udostępnianie**. Udostępnione zasoby są widoczne w otoczeniu sieciowym. Udostępnianie plików i drukarek można wyłączyć globalnie w **Centrum sieci i udostępniania** w Panelu Sterowania, a danego zasobu po kliknięciu prawym klawiszem myszki w Eksploratorze Plików i wybraniu opcji menu rozwijalnego: **Udostępnij | Zatrzymaj udostępnianie**.

Zadania

- Udostępnij folder Folder_d_g, w którym przechowywane są pliki tymczasowe.
- Sprawdzić adres IP na swoim komputerze i podać go sąsiadowi
- Tylko w XP!! W oknie Mój komputer w menu Opcje folderów w zakładce Widok plików włącz „proste udostępnianie”. Udostępnij Folder_d_g. Sprawdź u sąsiada, w jaki sposób jest on widoczny w sieci, a następnie wyłącz „proste udostępnianie”.
- Udostępnić Folder_d_g i przypisać następujące uprawnienia:
- dla Lab_d_g_11gr prawo tylko do odczytu
- dla Lab_d_g_12gr prawo pełnej kontroli
- Administratorzy – brak uprawnień (tzn. nie chodzi tutaj o uprawnienie Odmawiaj, po prostu w ogóle nie umieszczać grupy na liście)

- Zamapować udostępniony u partnera udział jako użytkownik Lab_d_g_11. Sprawdzić, czy można zmodyfikować plik plik.txt. Odłączyć udział
- Zamapować udostępniony u partnera udział jako użytkownik Lab_d_g_12. Sprawdzić, czy można zmodyfikować plik plik.txt. Sprawdzić, czy można usunąć plik plik.txt (lokalne prawo do usuwania).
- Odłączyć udział