

## 12.1 Zarządzanie zasadami grup w domenie

Przed przystąpieniem do ćwiczenia sprawdź i ustaw

W Menedżerze funkcji Hyper-V wybierz nazwa maszyny wirtualnej twojej grupy **\_dc2019**

**Upewnij się, że przywrócony punkt kontrolny, zawiera serwer z zainstalowanym kontrolerem domeny.**

Uruchom maszynę > Ctrl+Delete > Administrator > zaq1@WSX

a) system serwera są jak poniżej:

The screenshot shows the Windows Server Manager interface. The left pane displays the navigation tree with 'Serwer lokalny' selected. The right pane shows the 'WŁAŚCIWOŚCI' (Properties) for the local server. The 'Dla roli' (For roles) section is expanded, showing the following settings:

Ustawienie	Wartość
Nazwa komputera	rol
Domena	rol00.edu.pl
Zapora systemu Windows	Domena: Włączone
Zdalne zarządzanie	Włączone
Pulpit zdalny	Wyłączone
Tworzenie zespołu kart interfejsu sieciowego	Wyłączone
Ethernet	192.167.0.1, Protokół IPv6 włączony

Below the server manager, a network configuration window is shown for the 'Ethernet' adapter. It displays the following settings:

Ustawienie	Wartość
DHCP włączone	Nie
Adres IPv4	192.167.0.1
Maska podsieci IPv4	255.255.255.0
Brama domyślna IPv4	
Serwer DNS IPv4	192.167.0.1

Jeśli pracujesz w VirtualBox utwórz migawkę stanu systemu serwera o nazwie **DDMM\_numer**

b) systemu klienta są jak poniżej:

The screenshot shows the Windows network configuration settings. The 'Użyj następującego adresu IP:' (Use the following IP address) option is selected. The settings are as follows:

Ustawienie	Wartość
Adres IP:	192 . 167 . 0 . 21
Maska podsieci:	255 . 255 . 255 . 0
Brama domyślna:	192 . 167 . 0 . 1

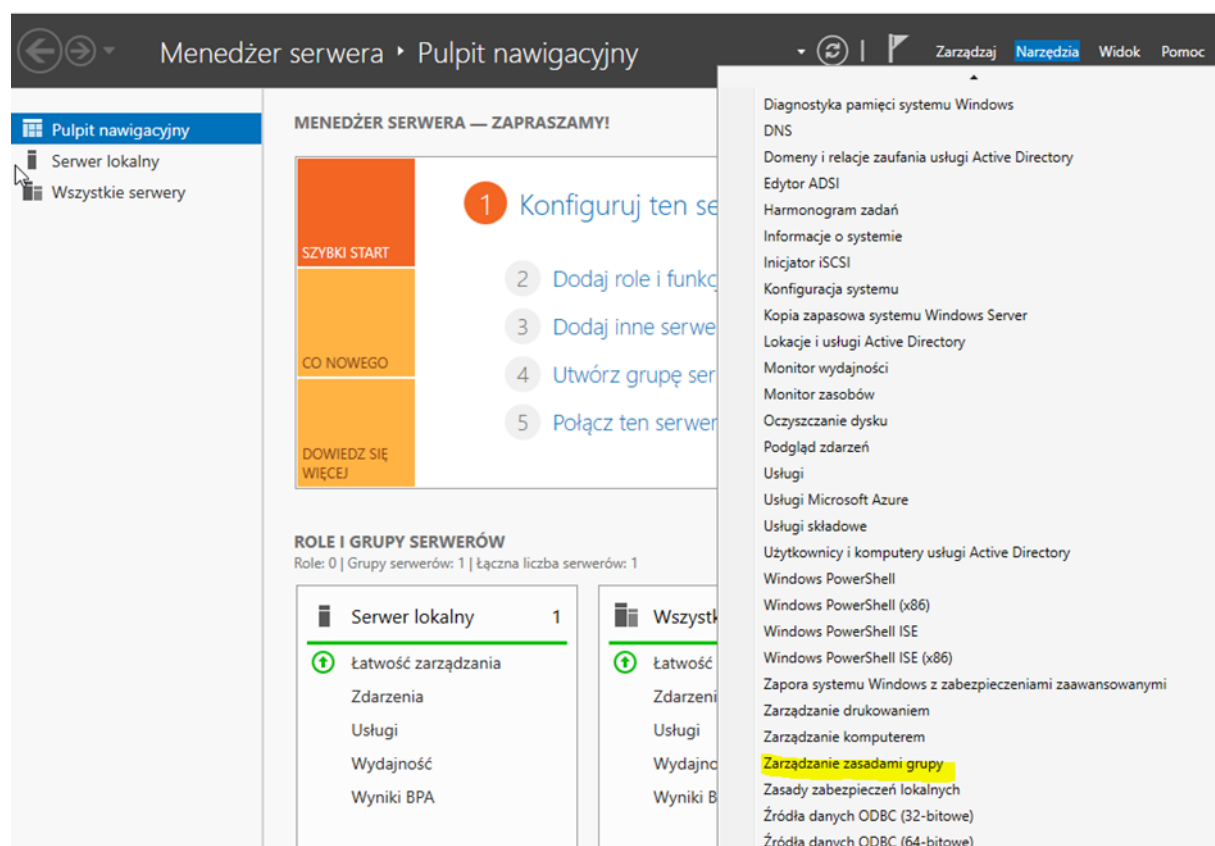
The 'Użyj następujących adresów serwerów DNS:' (Use the following DNS server addresses) option is also selected. The settings are as follows:

Ustawienie	Wartość
Preferowany serwer DNS:	192 . 167 . 0 . 1
Alternatywny serwer DNS:	.

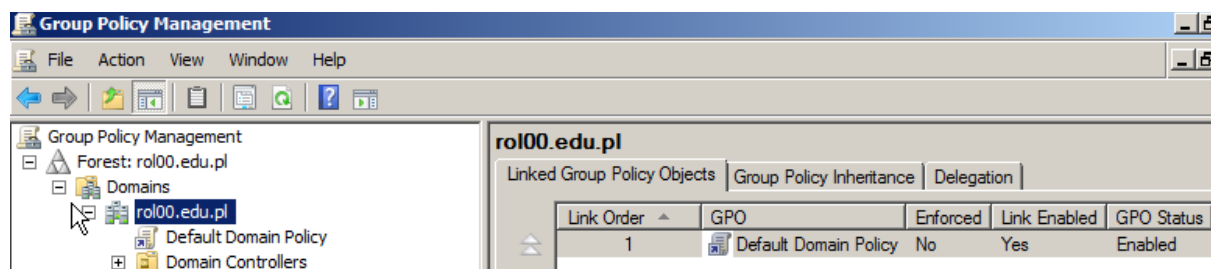
W zeszycie opisz procedury tworzenie zasad grup w domenie.

**Procedura tworzenia zasad grup.**

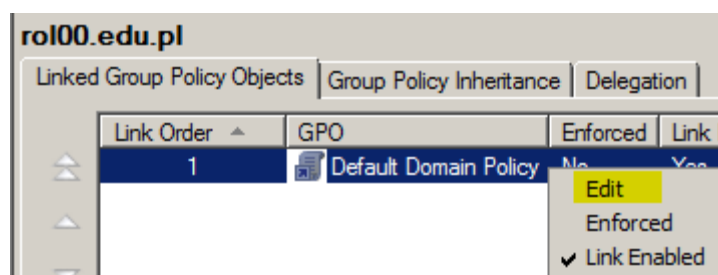
Konsola Group Policy Management (Zarządzanie zasadami grupy) jest zestawem programowalnych interfejsów służących do zarządzania zasadami grupy.



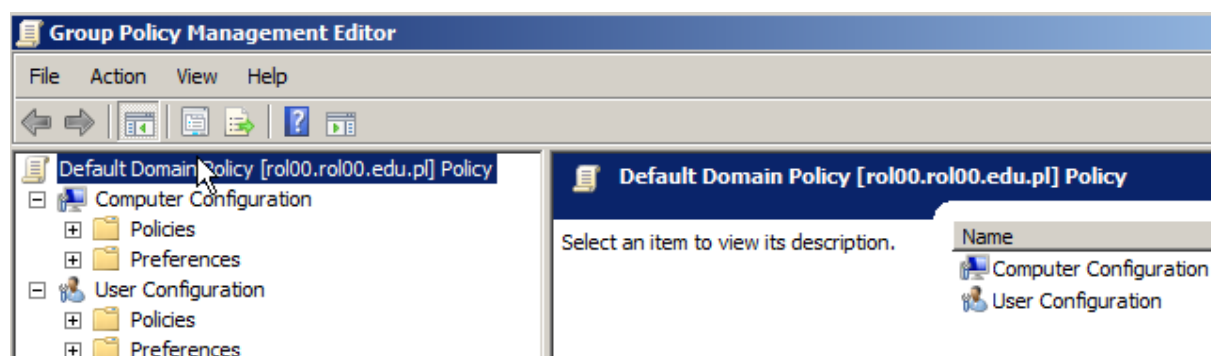
Konsola Group Policy Management (Zarządzanie zasadami grupy)



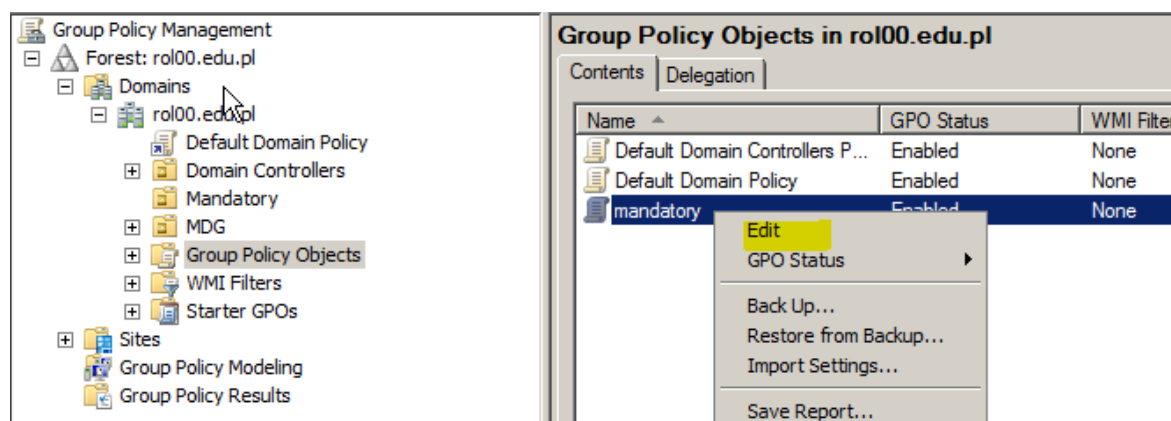
Gdy obiekty GPO zostaną zdefiniowane na poziomie domeny można zarządzać konfiguracją ustawień obejmujących całą domenę.



Konsola Group Policy Management nie zastępuje Edytora obiektów zasad grupy (Group Policy Object Editor). Edytowanie obiektów GPO nadal będzie się odbywało w tym edytorze.

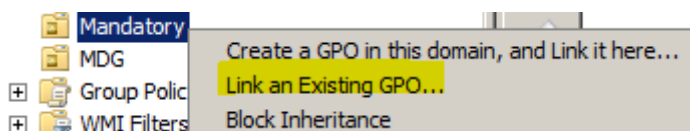


Grupując zestawy ustawień w odrębnych obiektach GPO, można zdefiniować inną konfigurację każdego obiektu GPO, tak aby każdy obiekt GPO miał wpływ tylko na wybrane konta komputerów oraz użytkowników. Po utworzeniu obiektu GPO trzeba skonfigurować jego ustawienia.



Co to jest łącze obiektu GPO?

Wszystkie obiekty GPO przechowywane są w usłudze Active Directory w kontenerze Group Policy Objects. Jeśli obiekt GPO jest używany przez lokację, domenę oraz jednostkę organizacyjną, obiekt ten ma łącze do kontenera Group Policy Objects. Dzięki temu można centralnie zarządzać i wdrażać obiekty GPO w wielu domenach oraz jednostkach organizacyjnych.



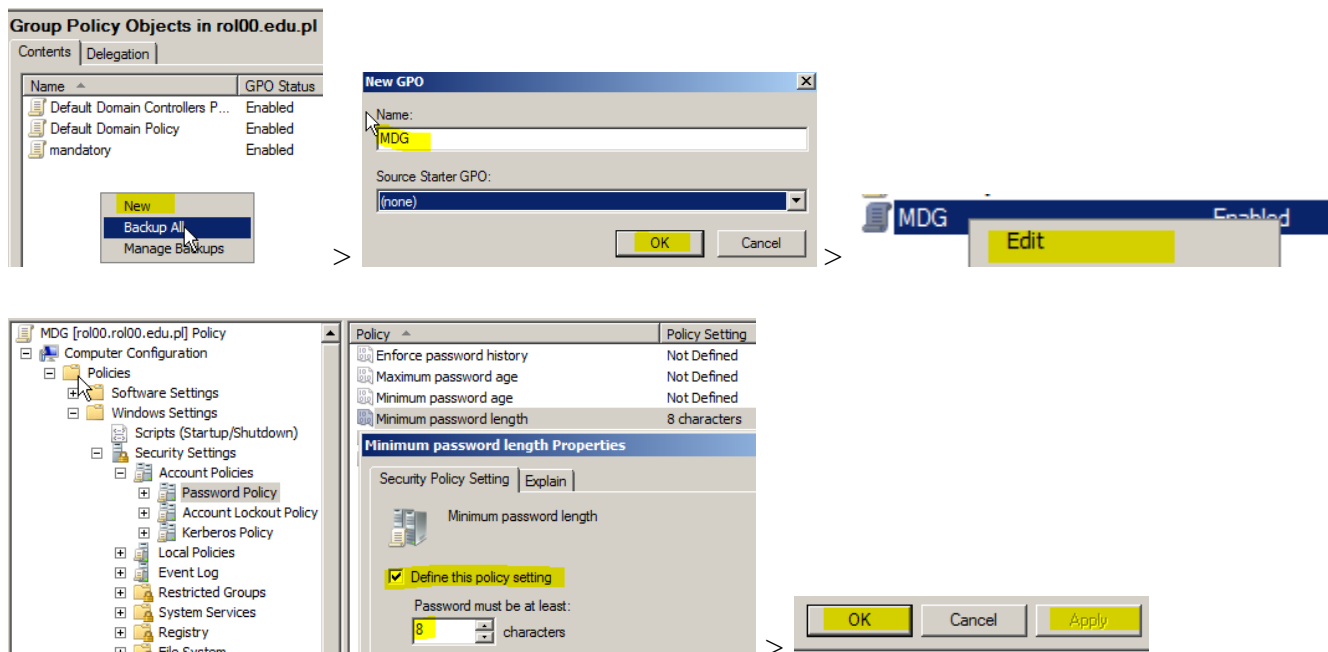
Jeśli obiekt GPO utworzony zostanie w kontenerze Group Policy Objects, ustawienia w nim skonfigurowane nie będą wdrażane do ustawień użytkowników i komputerów, dopóki nie zostanie utworzone łącze do tego obiektu GPO.

W konsoli Group Policy Management można również:

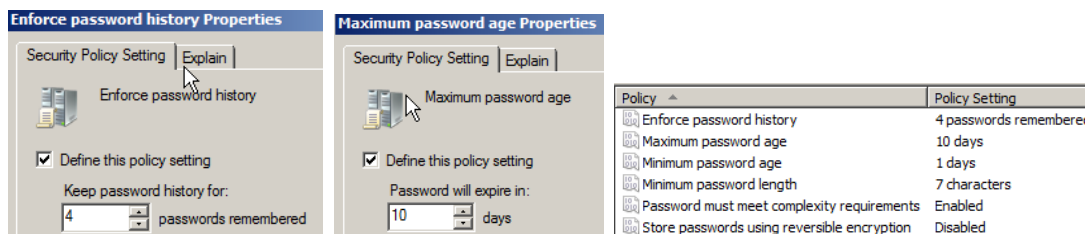
- tworzyć i przywracać kopie zapasowe obiektów GPO.
- kopiować i importować obiekty GPO.
- stosować filtry WMI (Windows Management Instrumentation).
- tworzyć raporty w oparciu o dane obiektów GPO i wynikowych zestawów zasad.
- wyszukiwać obiekty GPO.

Cele laboratorium

### Utworzenie zasady zabezpieczeń dla obiektów w kontenerze MDG



Minimum password length (Minimalna długość hasła) - to ustawienie zabezpieczeń określa najmniejszą liczbę znaków, jaką musi zawierać hasło do konta użytkownika. Można ustawić wartość z zakresu od 1 do 14 znaków lub określić, że hasło nie jest wymagane, wybierając jako liczbę znaków wartość 0.

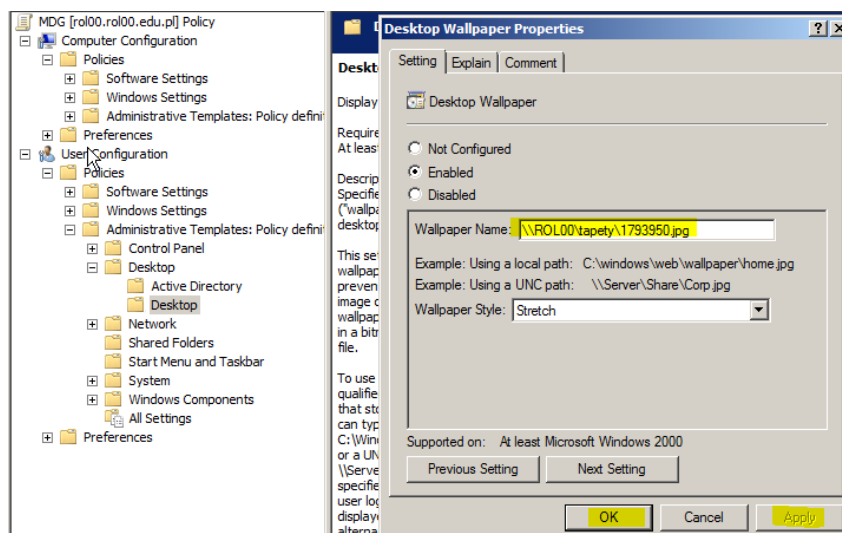


**Enforce password history (Wymuszaj tworzenie historii haseł)** - to ustawienie określa liczbę unikatowych nowych haseł, które muszą zostać przypisane kontu użytkownika, zanim będzie można ponownie użyć starego hasła. Wartość ta musi się zawierać w przedziale od 0 do 24 haseł. Zasada ta

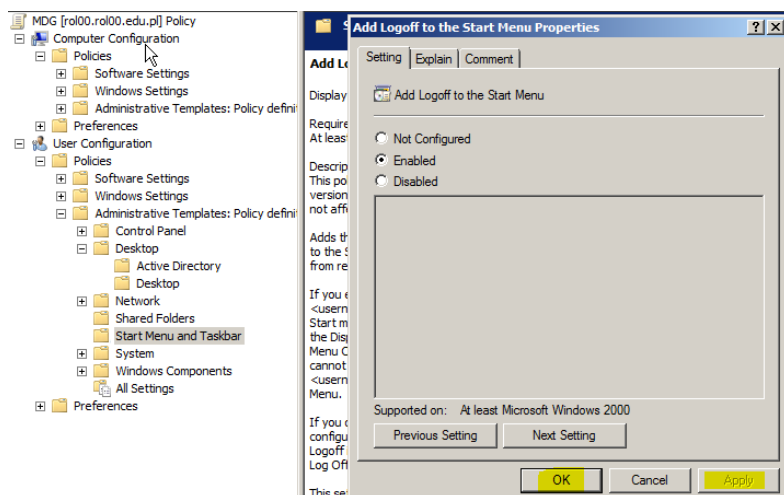
umożliwia administratorom podniesienie poziomu bezpieczeństwa, gdyż gwarantuje, że stare hasła nie będą stale w użyciu.

**Maximum password age (Maksymalny okres ważności hasła)** - określa okres (w dniach), w jakim można używać hasła, zanim system będzie wymagał jego zmiany. Można zmienić to ustawienie tak, aby hasła wygasły po określonej liczbie dni z przedziału od 1 do 999, albo określić, że hasła nigdy nie wygasają, ustawiając liczbę dni równą 0. Jeśli maksymalny okres ważności hasła mieści się w przedziale od 1 do 999 dni, wartość Minimalny okres ważności hasła musi być mniejsza od maksymalnego okresu ważności hasła. Jeśli maksymalnemu okresowi ważności hasła nadano wartość 0, minimalny okres ważności hasła może mieć dowolną wartość z przedziału od 0 do 998 dni.

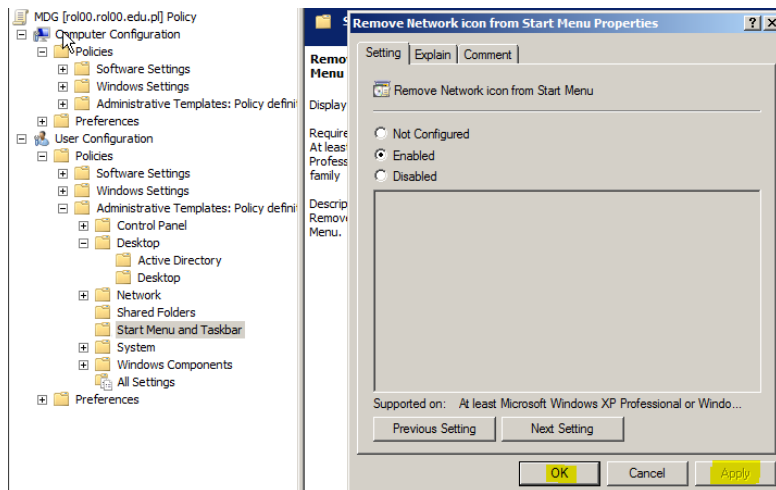
Uwaga: W trosce o maksymalne bezpieczeństwo należy wymusić wygasanie haseł co 30 lub 90 dni, w zależności od środowiska. Dzięki temu atakujący ma ograniczony czas na złamanie hasła użytkownika i uzyskanie dostępu do zasobów sieciowych. Domyślnie: 42.



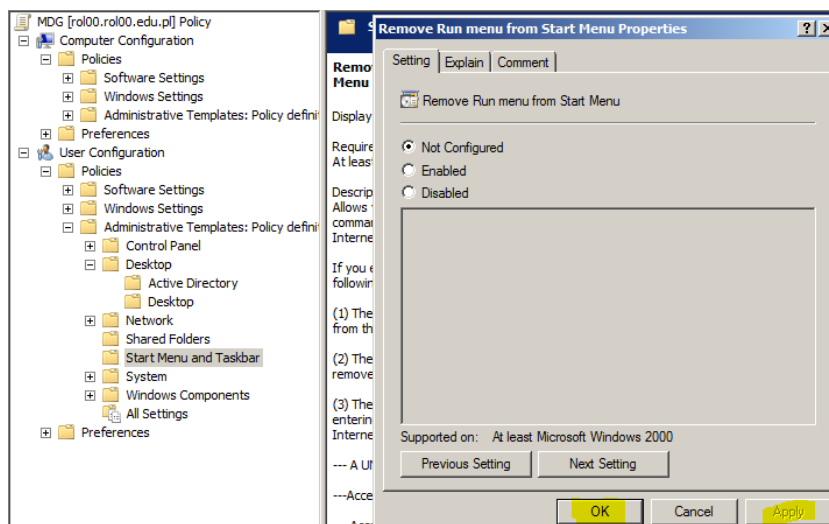
Ustawienie lokalizacji sieciowej tapety pulpitu (Desktop Wallpaper)



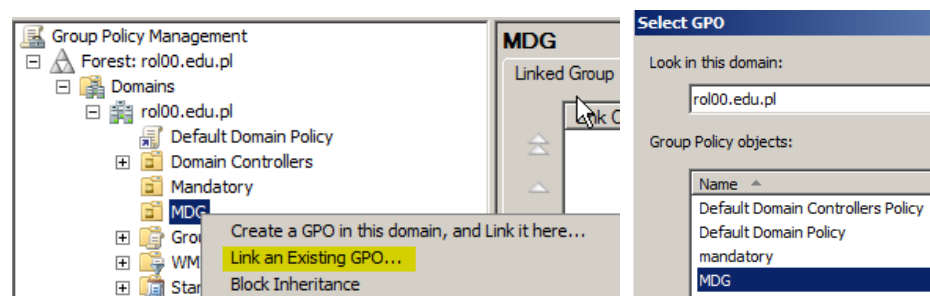
## Dodaj wylogowanie do menu Start



## Usuń ikonę Sieć z menu Start



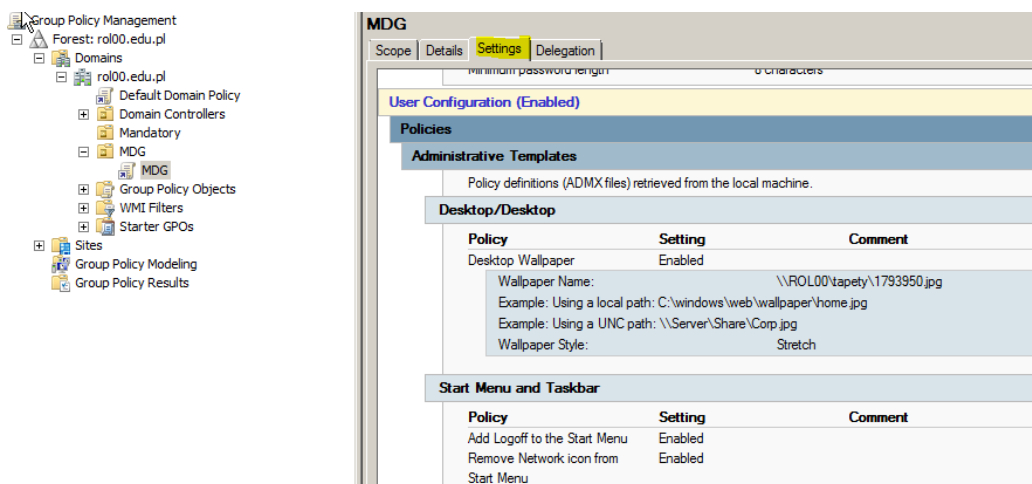
## Usuń menu Uruchom z menu Start



## Powiąz istniejący GPO ...

MDG			
Linked Group Policy Objects    Group Policy Inheritance    Delegation			
This list does not include any GPOs linked to sites. For more details, see Help.			
Precedence	GPO	Location	GPO Status
1	MDG	MDG	Enabled
2	Default Domain Policy	rol00.edu.pl	Enabled

## Wyświetla ustawienia

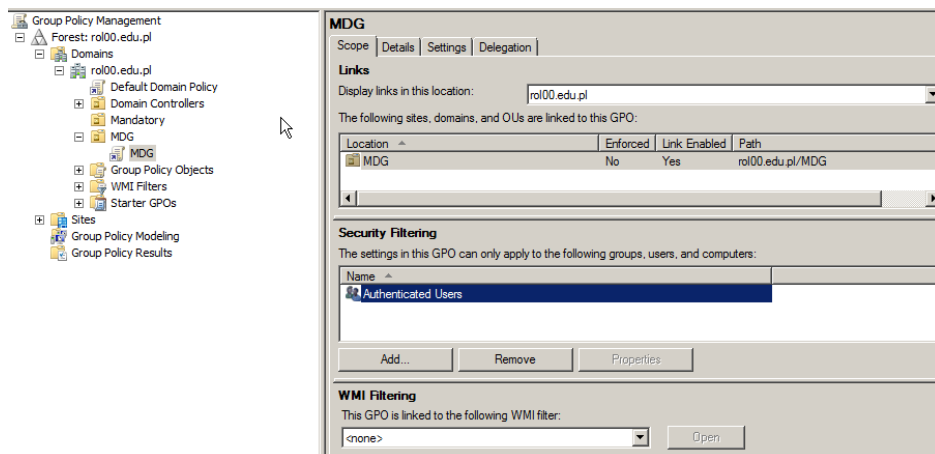


The screenshot shows the Group Policy Management console. In the left pane, the hierarchy is: Forest: rol00.edu.pl > Domains > MDG. The right pane displays the 'Settings' tab for the MDG GPO. It shows 'User Configuration (Enabled)' and 'Administrative Templates'. Under 'Desktop/Desktop', there is a table with the following data:

Policy	Setting	Comment
Desktop Wallpaper	Enabled	

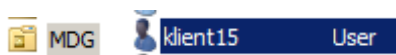
Below this, there is a section for 'Start Menu and Taskbar' with a similar table structure.

## Wyświetl zakres stosowania zasad

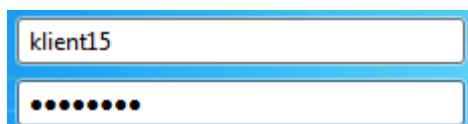


The screenshot shows the 'Links' tab for the MDG GPO. The 'Display links in this location' is set to 'rol00.edu.pl'. The 'Security Filtering' section shows 'Authenticated Users' selected. The 'WMI Filtering' section shows 'none' selected.

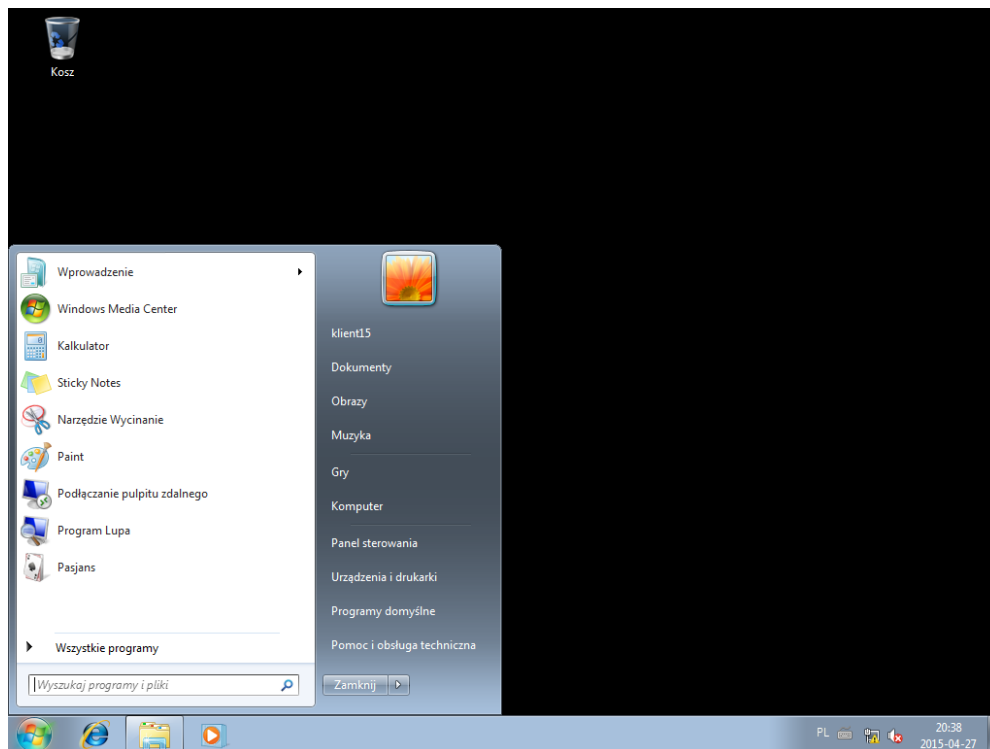
Upewnij się że istnieje w jednostce organizacyjnej **MDG** konto **klient15**



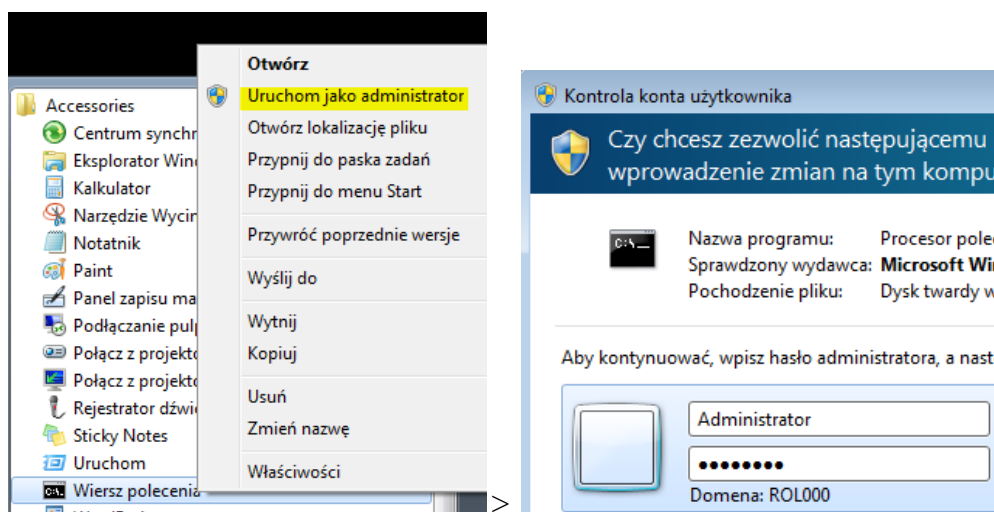
Na maszynie klienckiej zaloguj się do konta **klient15**



Efekt:



Uruchom wiersz polecenia jako administrator



Odśwież zasady zabezpieczeń - `gpupdate /force`



```
Administrator: \\ROL00\Profiles$\klient15\Start Menu\Programs\Accessories\Command Prompt.Ink...

C:\Windows\system32>gpupdate /force
Trwa aktualizowanie zasad...

Aktualizacja zasad użytkownika została ukończona pomyślnie.

Podczas przetwarzania zasad użytkownika napotkano następujące ostrzeżenia:

Rozszerzenie po stronie klienta zasad grupy Folder Redirection nie mogło zastosować co najmniej jednego ustawienia, ponieważ zmiany muszą być przetworzone przed uruchomieniem systemu lub zalogowaniem się użytkownika. Przed następnym uruchomieniem lub zalogowaniem się tego użytkownika system będzie czekać na całkowite zakończenie przetwarzania zasad grupy. Może to spowodować obniżenie wydajności uruchamiania i rozruchu. Administratorzy systemu mogą skonfigurować to rozszerzenie zasad grupy w taki sposób, aby uniknąć tych opóźnień lub zmniejszyć częstość ich występowania.
Aktualizacja zasad komputera została ukończona pomyślnie.

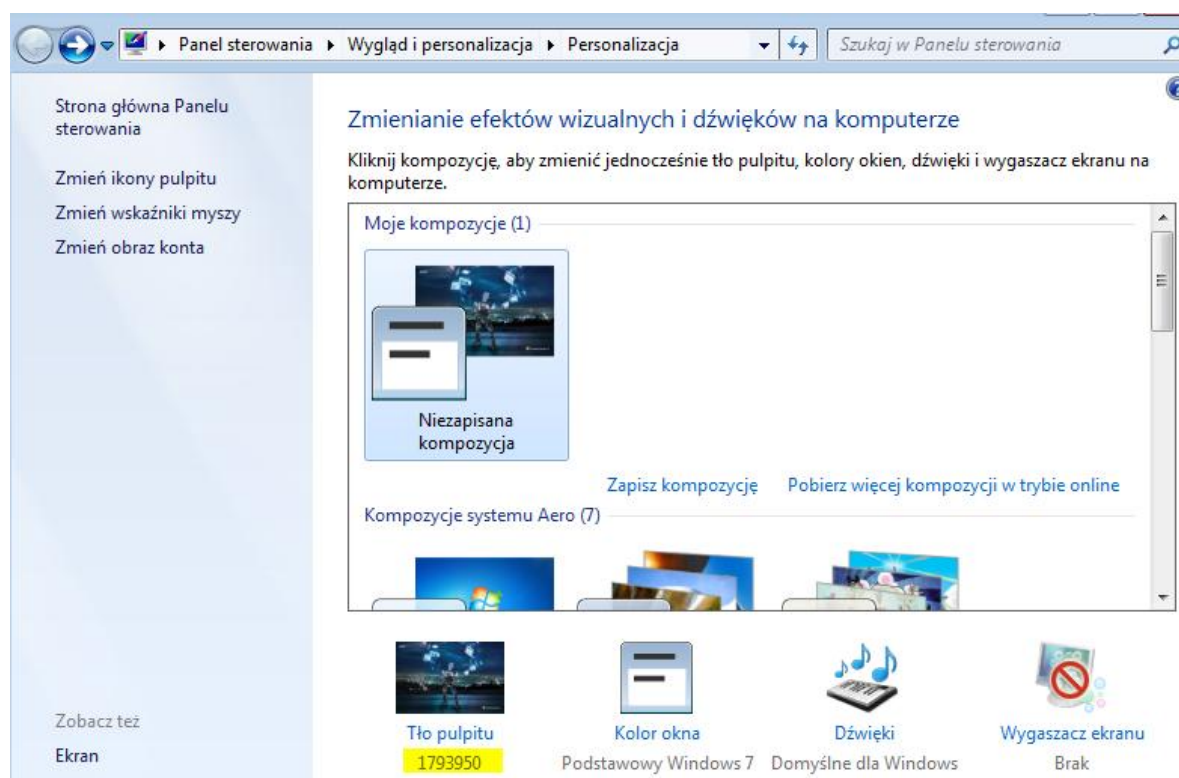
Aby uzyskać szczegółowe informacje, przejrzyj dziennik zdarzeń lub uruchom w wierszu poleceń polecenie GPRESULT /H GPREport.html w celu uzyskania dostępu do informacji o wynikach zasad grupy.

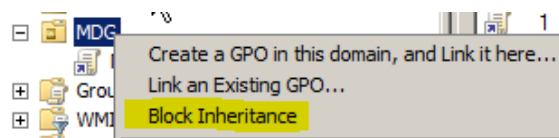
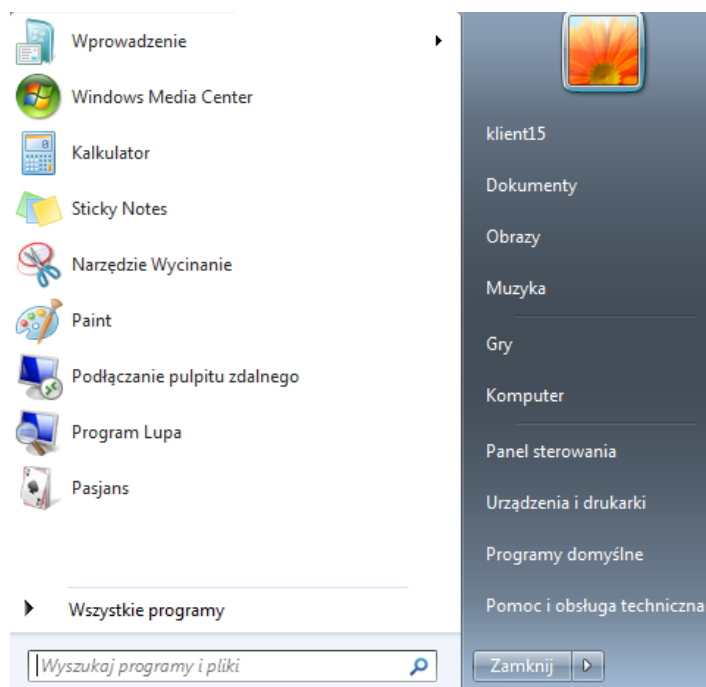
Uruchamianie pewnych zasad użytkownika jest włączone tylko podczas logowania.

Czy można przeprowadzić wylogowanie? <T/N>t
```

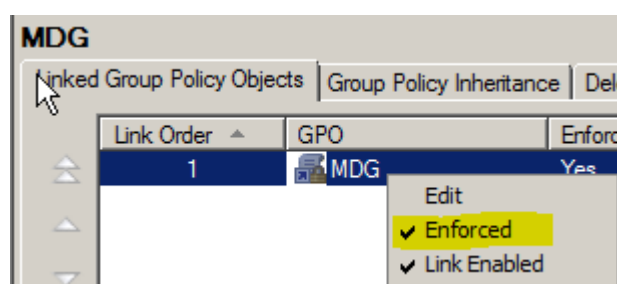
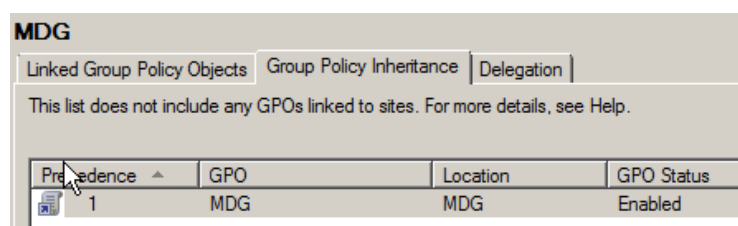
Na maszynie klienckiej zaloguj się do konta rol00\klient15

Efekt





Włącz na poziomie jednostki organizacyjnej „Block Inheritance” (Zablokuj dziedziczenie).



Włącz na poziomie zasady zabezpieczeń MDG Enforced, Link Enable (Wymuszone, Łącze Włączone).

Druga część notatki.

Zapisz w zeszycie jakie ustawienia zasad zostały zastosowane na stacji roboczej.