

12.1 Zarządzanie zasadami grup w domenie

Ogólnym celem tej lekcji z języka polskiego jest nauka zarządzania politykami grupowymi w domenie.

Szczegółowe cele obejmują:

1. Sprawdzanie i konfigurowanie systemów serwera i klienta przed rozpoczęciem ćwiczenia.
2. Opisanie procedur tworzenia polityk grupowych w domenie.
3. Zrozumienie konsoli zarządzania politykami grupowymi oraz sposobu tworzenia i zarządzania obiektami polityk grupowych (GPO).
4. Wyjaśnienie, co oznacza link GPO i jak go używać do centralnego zarządzania GPO w wielu domenach i jednostkach organizacyjnych.
5. Nauka tworzenia polityk zabezpieczeń dla obiektów w kontenerze MDG, w tym ustawianie minimalnej długości hasła, wymuszanie historii haseł oraz ustawianie maksymalnego wieku hasła.

Przed przystąpieniem do ćwiczenia sprawdź i ustaw

W Menedżer funkcji Hyper-V wybierz nazwa maszyny wirtualna 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 configuration interface. The main window is titled "Menedżer serwera" and "Serwer lokalny". The "WŁAŚCIWOŚCI" (Properties) window is open, showing the following settings:

Property	Value
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 main window, the network configuration for the Ethernet adapter is shown:

Property	Value
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:

Użyj następującego adresu IP:

Adres IP: 192 . 167 . 0 . 21

Maska podsieci: 255 . 255 . 255 . 0

Brama domyślna: 192 . 167 . 0 . 1

Użyj następujących adresów serwerów DNS:

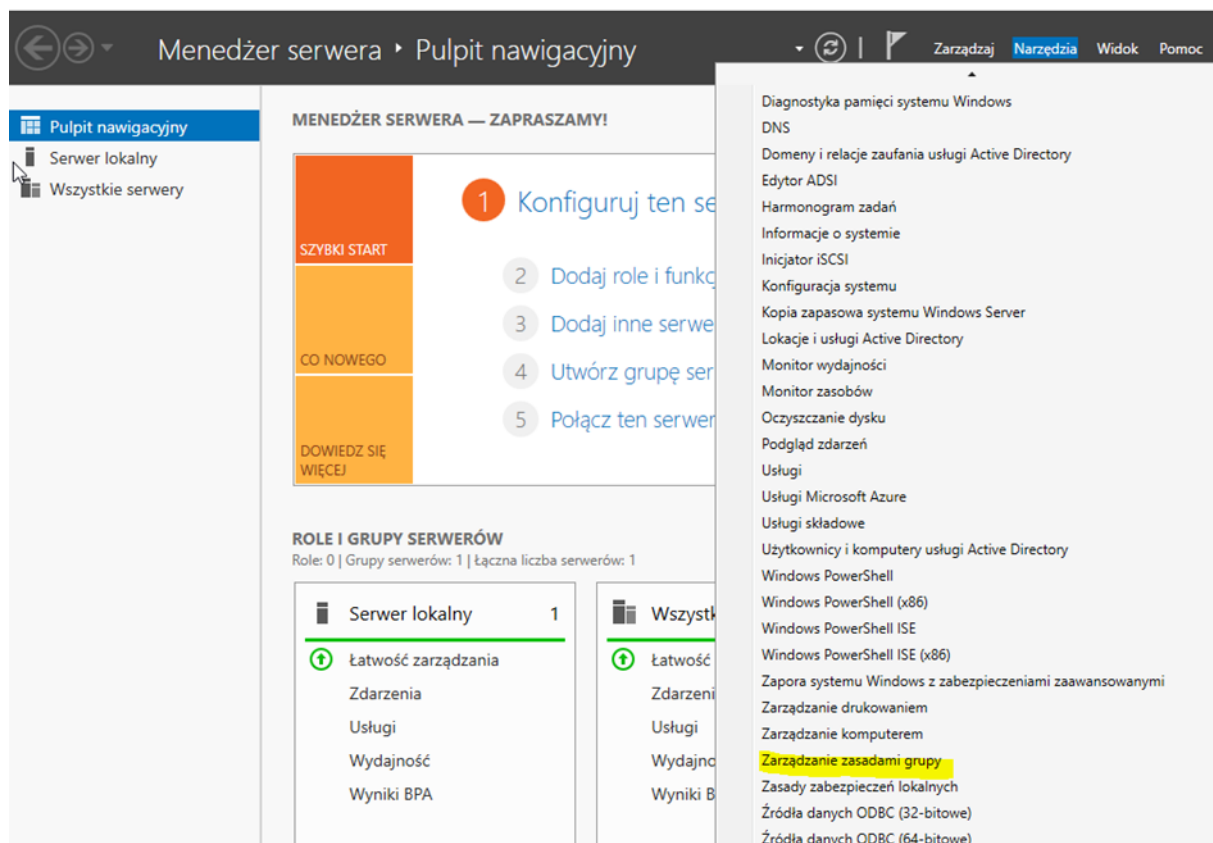
Preferowany serwer DNS: 192 . 167 . 0 . 1

Alternatywny serwer DNS: . . .

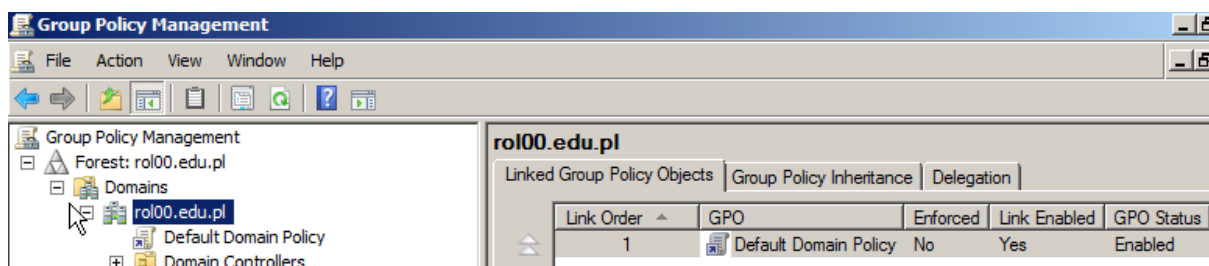
W zeszycie opisz procedury tworzenie zasad grup w domenie.

Procedura tworzenia zasad grup.

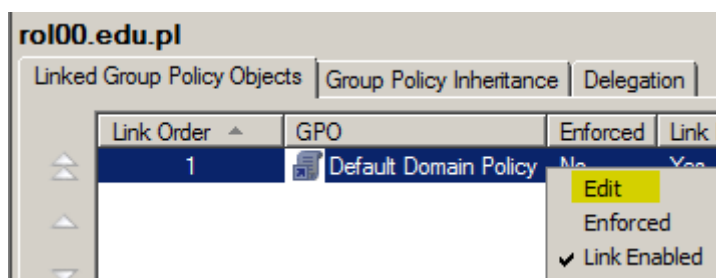
Konsola Group Policy Management (Zarządzanie zasadami grupy) jest zestawem programowalnych interfejsów służących do zarządzania zasadami grupy.



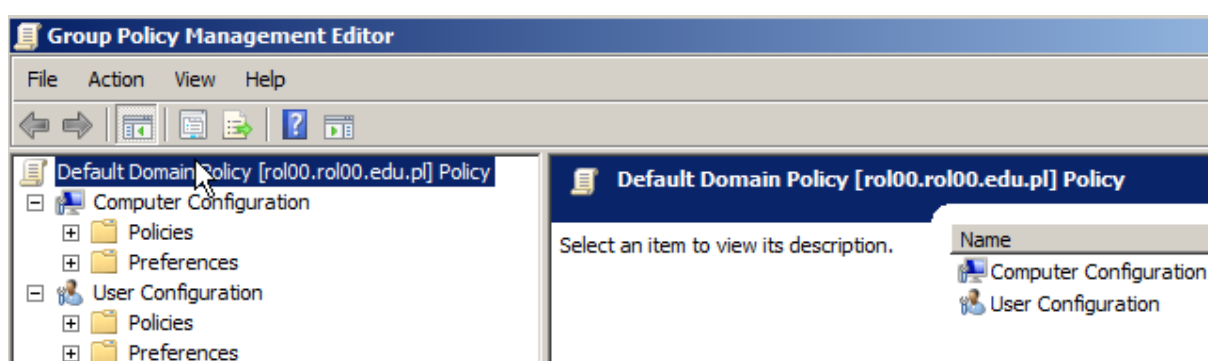
Konsola Group Policy Management (Zarządzanie zasadami grupy)



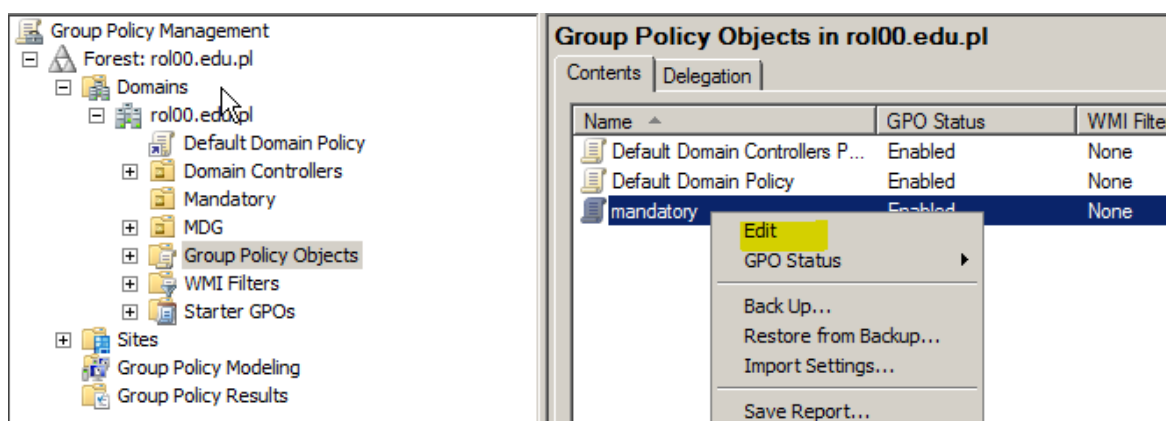
Gdy obiekty GPO zostaną zdefiniowane na poziomie domeny można zarządzać konfiguracją ustawień obejmujących całą domenę.



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

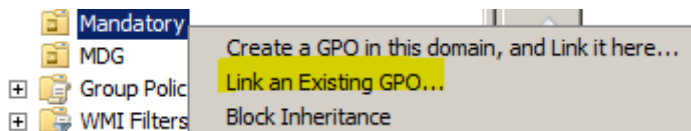


Grupując zestawy ustawień w odrębnych obiektach GPO, można zdefiniować inną konfigurację każdego obiektu GPO, tak aby każdy obiekt GPO miał wpływ tylko na wybrane konta komputerów oraz użytkowników. Po utworzeniu obiektu GPO trzeba skonfigurować jego ustawienia.



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.



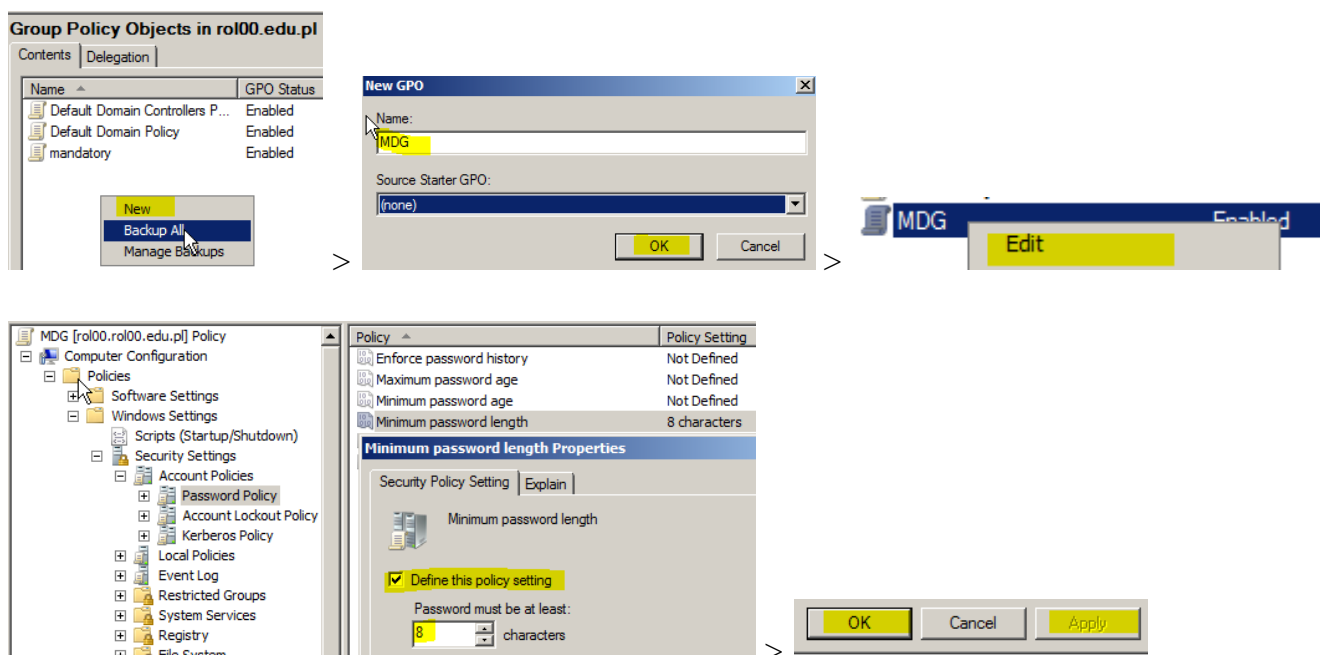
Jeśli obiekt GPO utworzony zostanie w kontenerze Group Policy Objects, ustawienia w nim skonfigurowane nie będą wdrażane do ustawień użytkowników i komputerów, dopóki nie zostanie utworzone łącze do tego obiektu GPO.

W konsoli Group Policy Management można również:

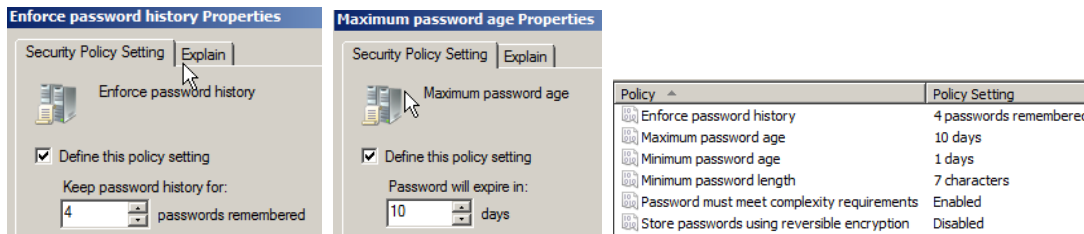
- tworzyć i przywracać kopie zapasowe obiektów GPO.
- kopiować i importować obiekty GPO.
- stosować filtry WMI (Windows Management Instrumentation).
- tworzyć raporty w oparciu o dane obiektów GPO i wyników zestawów zasad.
- wyszukiwać obiekty GPO.

Cele laboratorium

Utworzenie zasady zabezpieczeń dla obiektów w kontenerze MDG



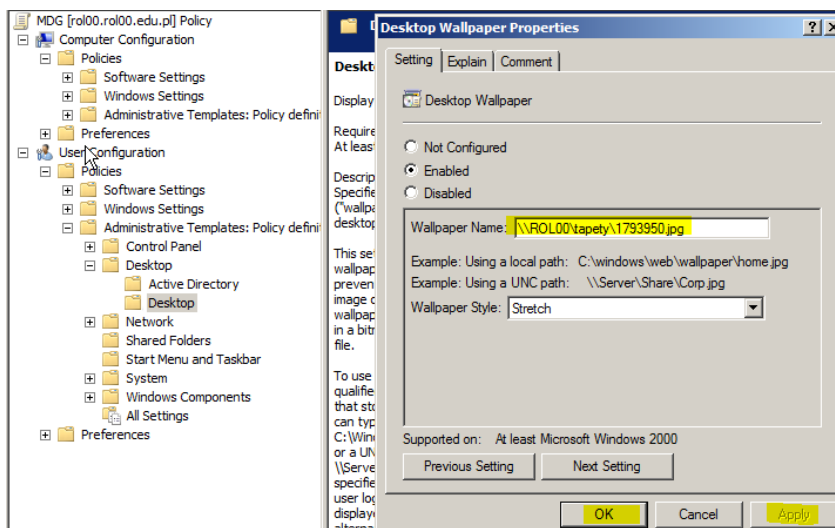
Minimum password length (Minimalna długość hasła) - to ustawienie zabezpieczeń określa najmniejszą liczbę znaków, jaką musi zawierać hasło do konta użytkownika. Można ustawić wartość z zakresu od 1 do 14 znaków lub określić, że hasło nie jest wymagane, wybierając jako liczbę znaków wartość 0.



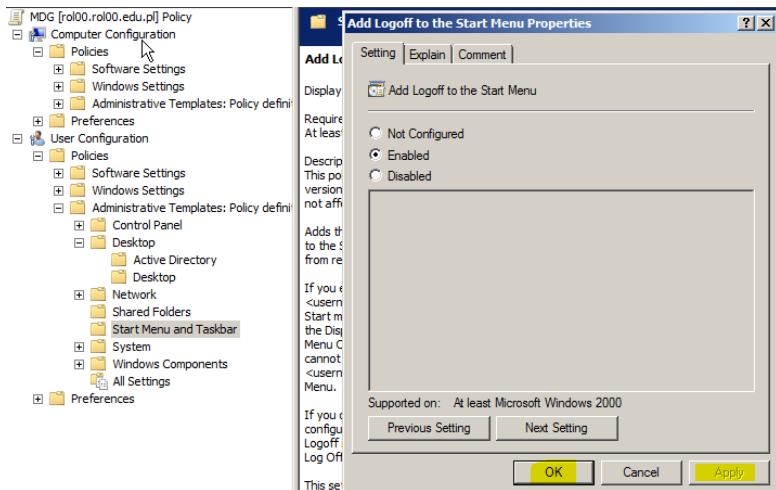
Enforce password history (Wymuszaj tworzenie historii haseł) - to ustawienie określa liczbę unikatowych nowych haseł, które muszą zostać przypisane kontu użytkownika, zanim będzie można ponownie użyć starego hasła. Wartość ta musi się zawierać w przedziale od 0 do 24 haseł. Zasada ta umożliwia administratorom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

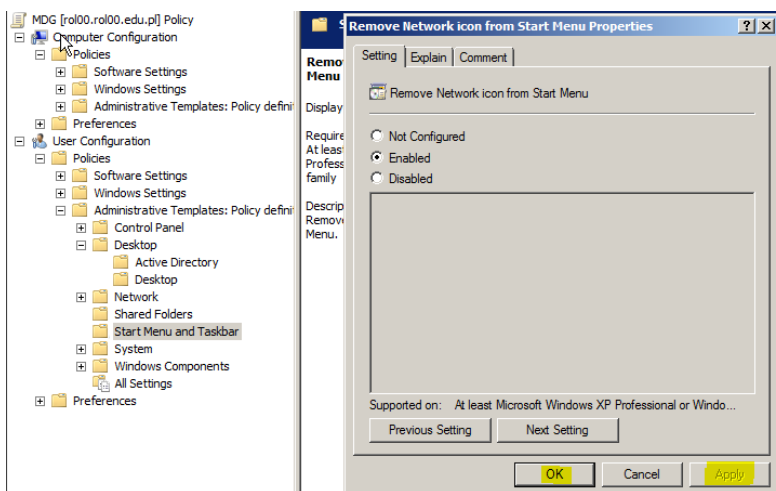
Uwaga: W trosce o maksymalne bezpieczeństwo należy wymusić wygasanie haseł co 30 lub 90 dni, w zależności od środowiska. Dzięki temu atakujący ma ograniczony czas na złamanie hasła użytkownika i uzyskanie dostępu do zasobów sieciowych. Domyślnie: 42.



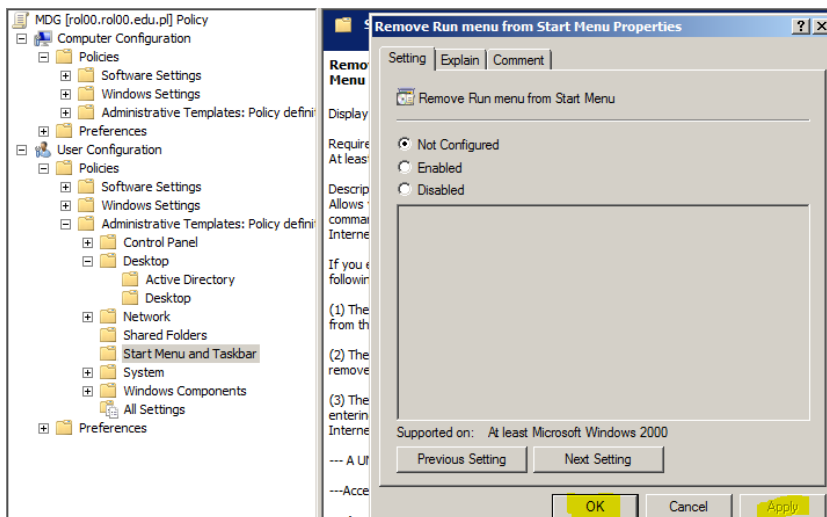
Ustawienie lokalizacji sieciowej tapety pulpitu (Desktop Wallpaper)



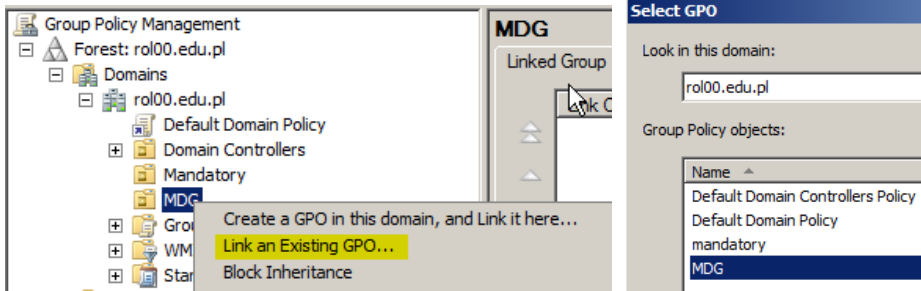
Dodaj wylogowanie do menu Start



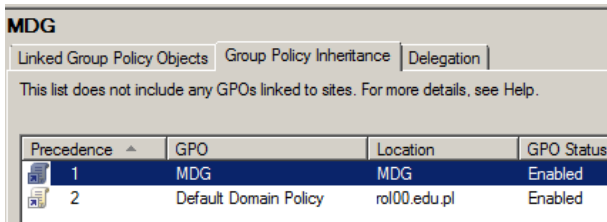
Usuń ikonę Sieć z menu Start



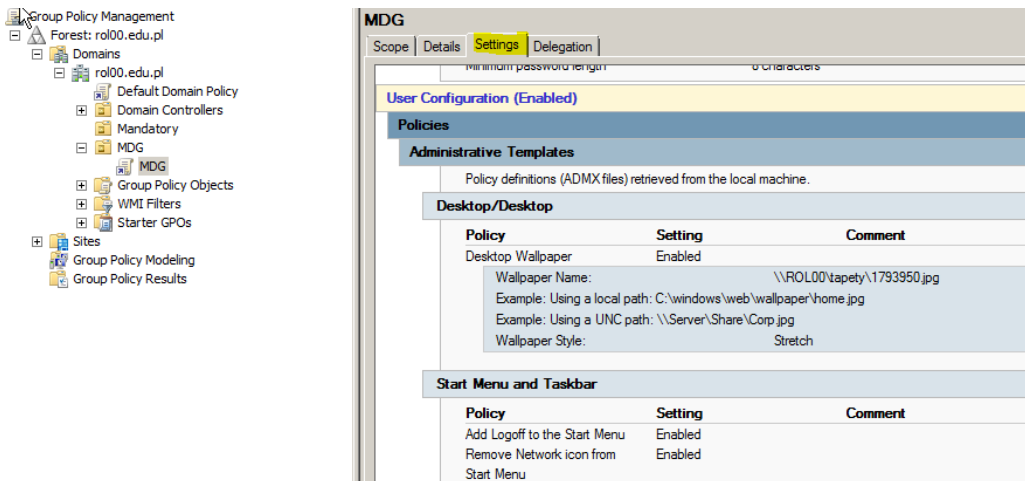
Usuń menu Uruchom z menu Start



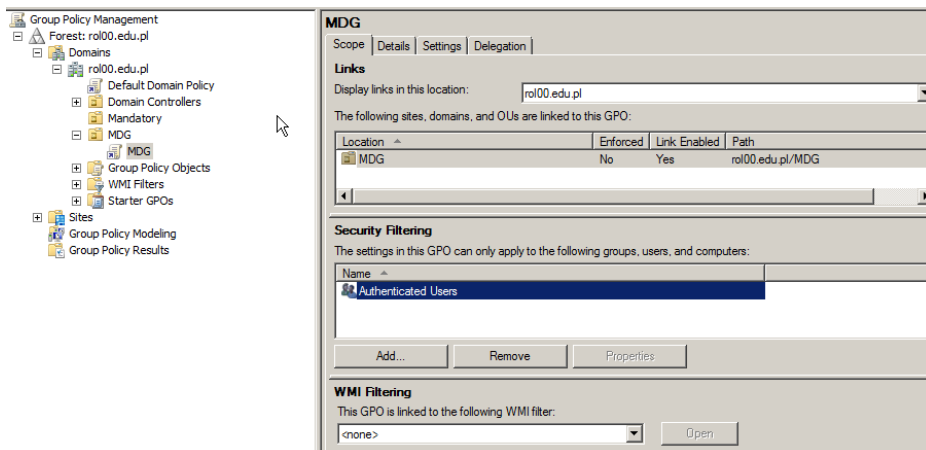
Powiąz istniejący GPO ...



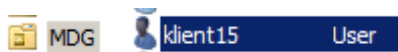
Wyświetla ustawienia



Wyświetl zakres stosowania zasad



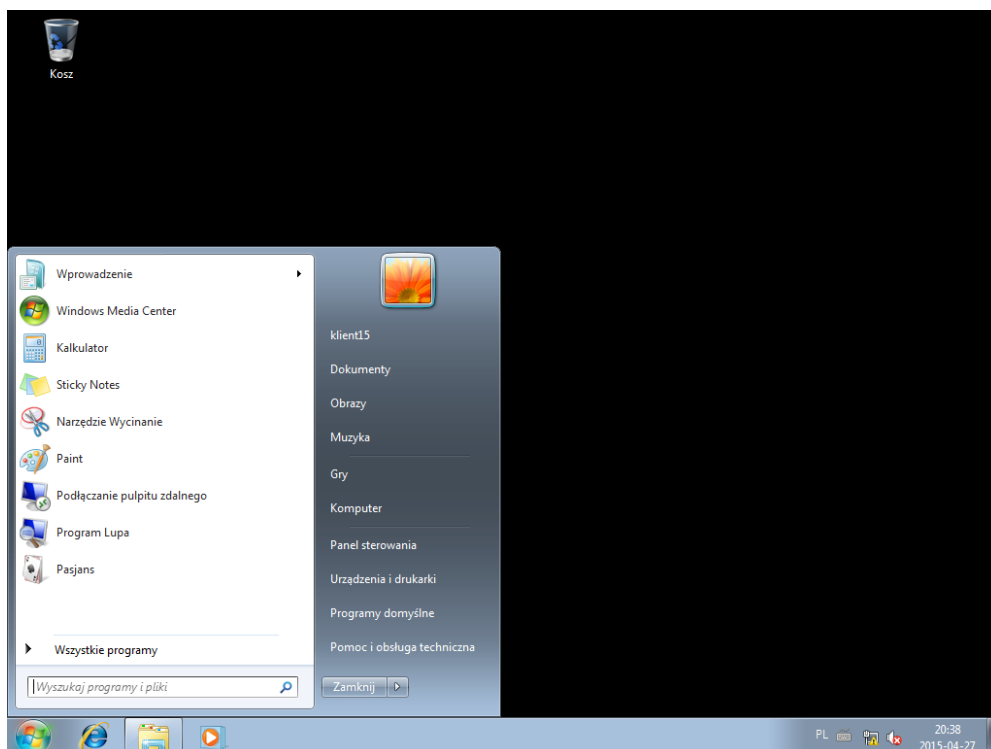
Upewnij się że istnieje w jednostce organizacyjnej MDG konto klient15



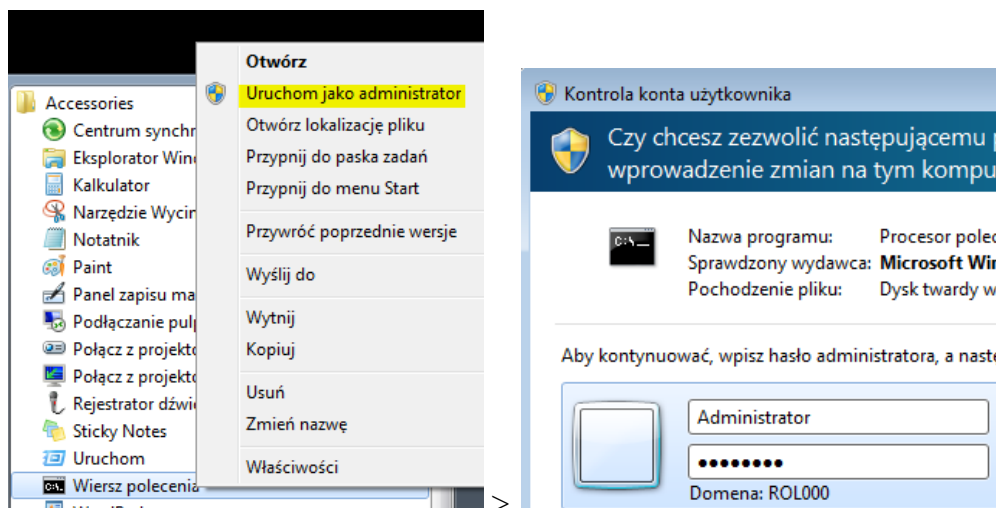
Na maszynie klienckiej zaloguj się do konta klient15



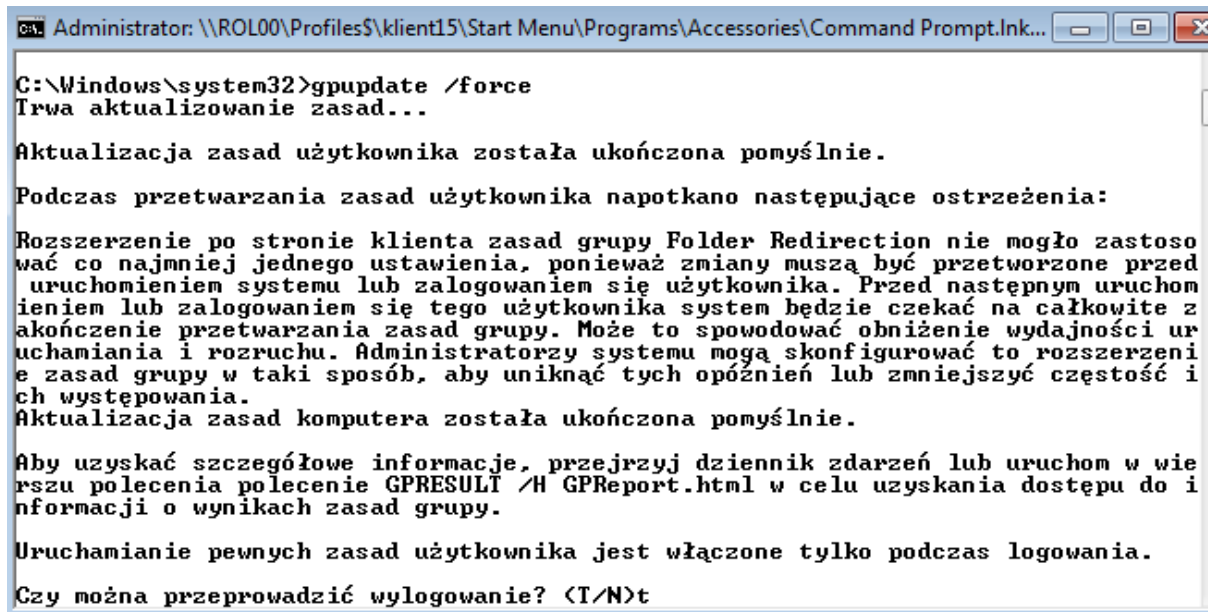
Efekt:



Uruchom wiersz polecenia jako administrator

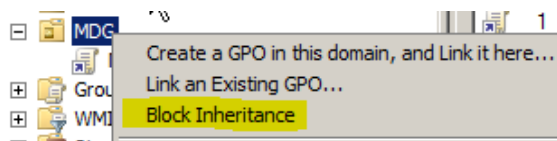


Odśwież zasady zabezpieczeń - `gpupdate /force`

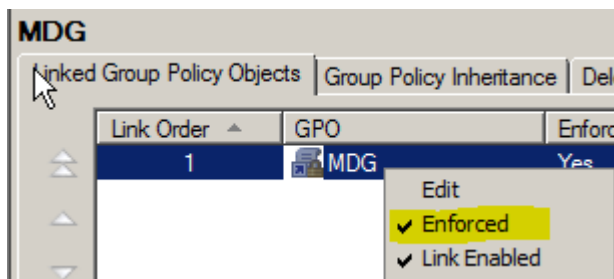
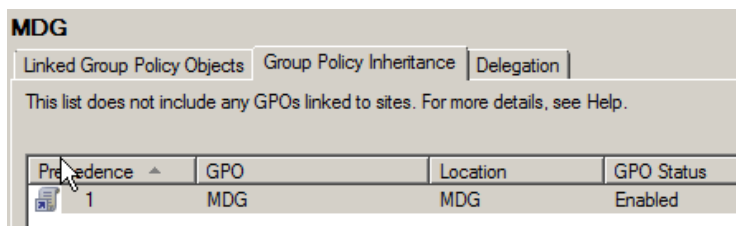


Na maszynie klienckiej zaloguj się do konta rol00\klient15

Na serwerze:



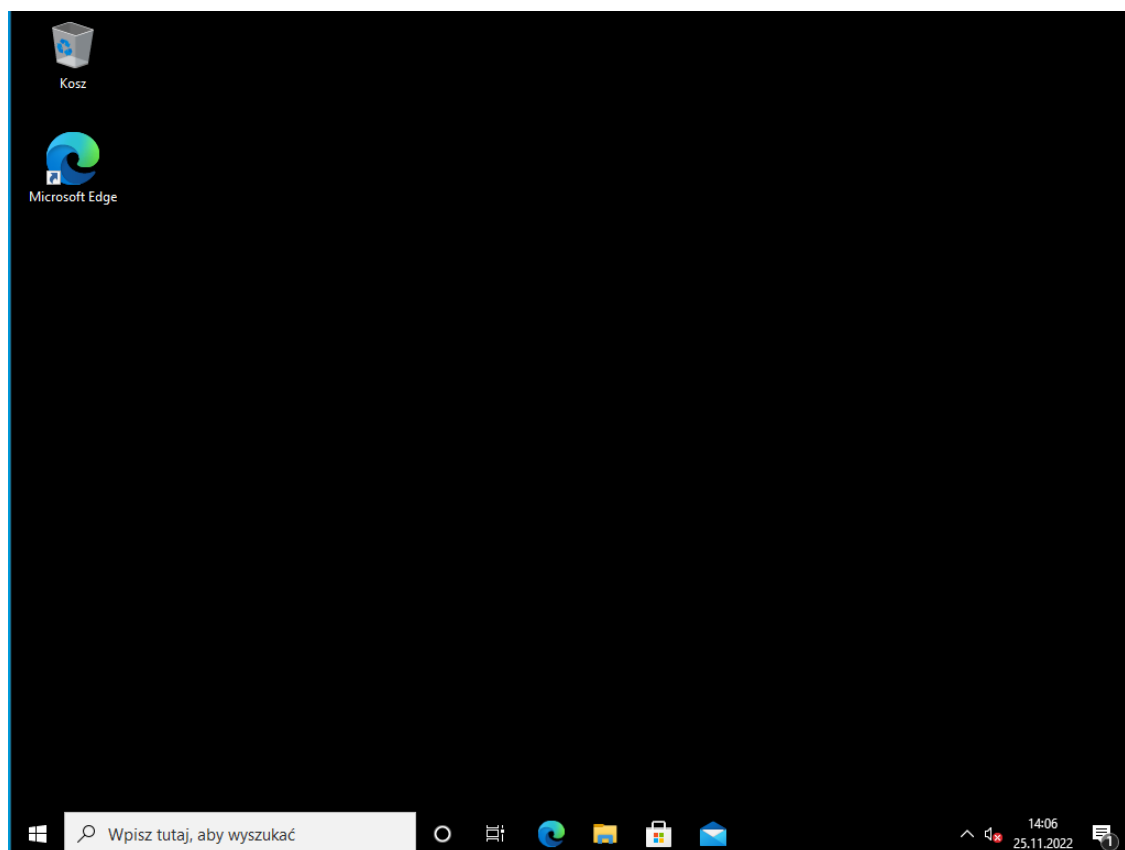
Włącz na poziomie jednostki organizacyjnej „Block Inheritance” (Zablokuj dziedziczenie).



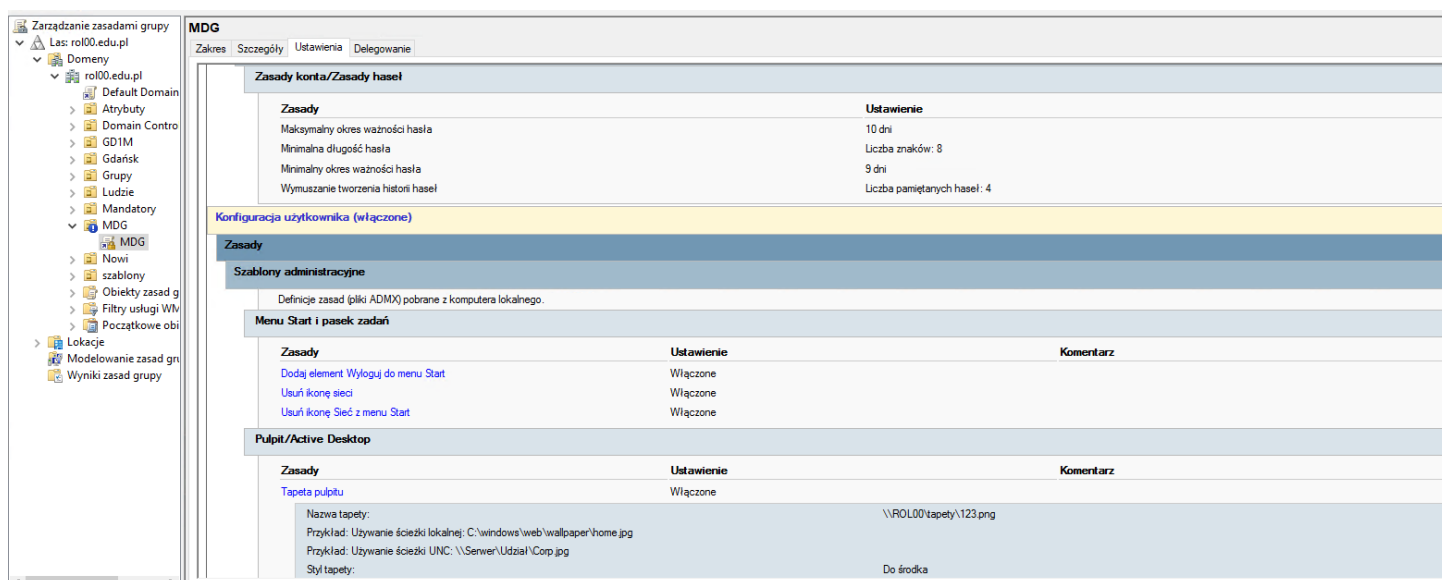
Włącz na poziomie zasady zabezpieczeń MDG Enforced, Link Enable (Wymuszone, Łącze Włączone).

Na maszynie klienckiej zalogowanej do konta rol00\klient15

Efekt końcowy:



Klient widok pulpitu.



Zarządzanie zasadami grupy > MDG > MDG > Ustawienia.

Druga część notatki.

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

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonanie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.