

12.3 Konfigurowanie zakresu zasad grup, obsługa zasad grup.

Przed przystąpieniem do ćwiczenia sprawdź i ustaw

W Menedżer funkcji Hyper-V wybierz nazwa maszyny wirtualna twojej grupy **_dc2019**

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

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

Przed przystąpieniem do ćwiczenia sprawdź i ustaw, jeśli to konieczne

a) system serwera są jak poniżej:

The screenshot shows the Windows Server Management console. The left pane shows the navigation tree with 'Serwer lokalny' selected. The right pane shows the 'Właściwości' (Properties) for the role 'rol'. The properties are as follows:

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 screenshot, a network configuration path is shown: > Adres IPv4 > Ethernet > Sieć niezidentyfikowana Intel(R) PRO/1000 MT Desktop Ad > Właściwości > DHCP włączone > Nie > Adres IPv4 > 192.167.0.1 > Maska podsieci IPv4 > 255.255.255.0 > Brama domyślna IPv4 > 192.167.0.1 > 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 client network configuration interface. The 'Użyj następującego adresu IP' (Use the following IP address) radio button is selected. The configuration is as follows:

Property	Value
Adres IP:	192 . 167 . 0 . 21
Maska podsieci:	255 . 255 . 255 . 0
Brama domyślna:	192 . 167 . 0 . 1

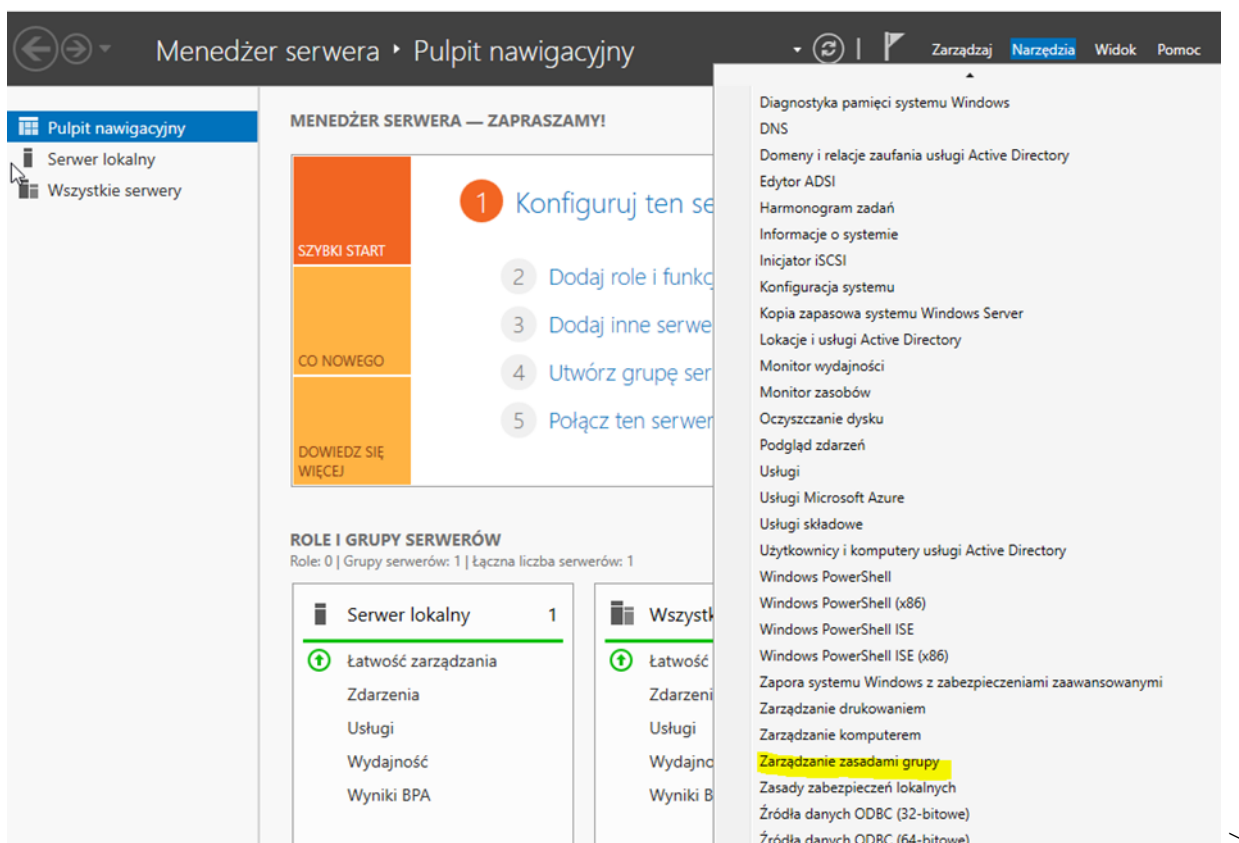
The 'Użyj następujących adresów serwerów DNS' (Use the following DNS server addresses) radio button is also selected. The configuration is as follows:

Property	Value
Preferowany serwer DNS:	192 . 167 . 0 . 1
Alternatywny serwer DNS:	.

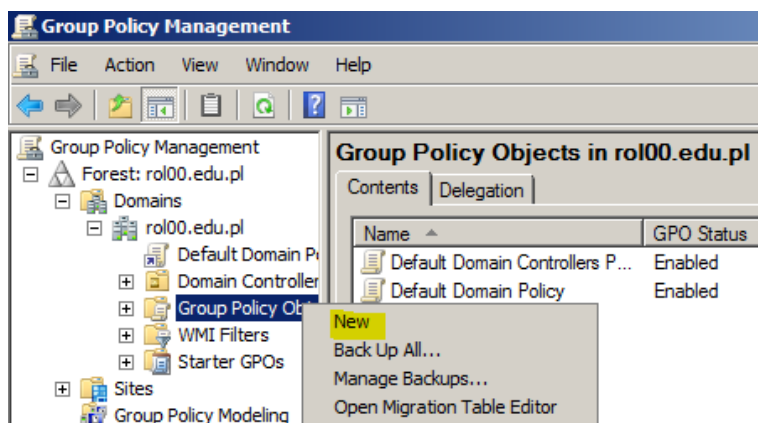
W zeszycie opisz procedury tworzenie zasad grup w domenie.

Zadanie 1

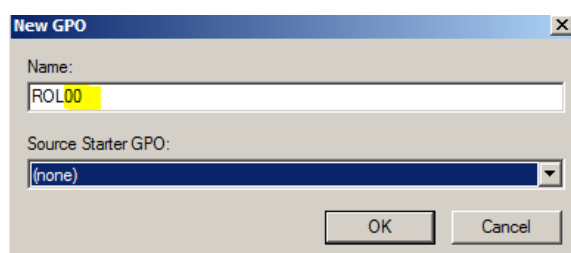
Procedura tworzenia, edycji i definiowania zakresu obiektu zasad grup.



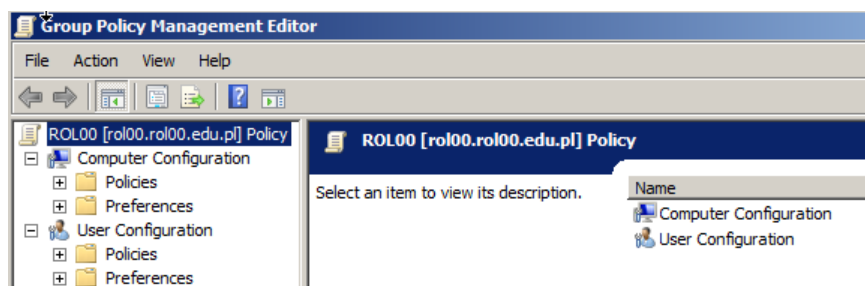
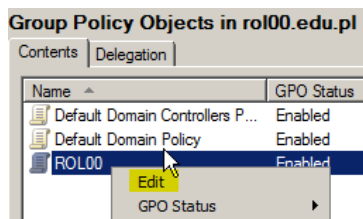
Kliknij prawym przyciskiem myszy kontener Group Policy Objects (Obiekty zasad grupy) w drzewie konsoli i wybierz New (Nowe).



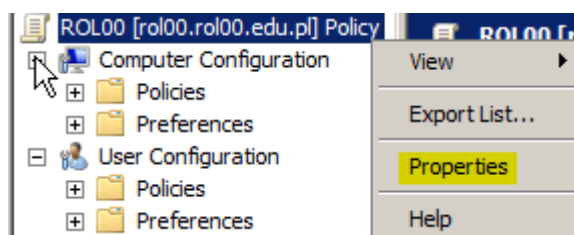
W polu Name (Nazwa) wpisz ROL00 gdzie 00 jest numerem twojego stanowiska



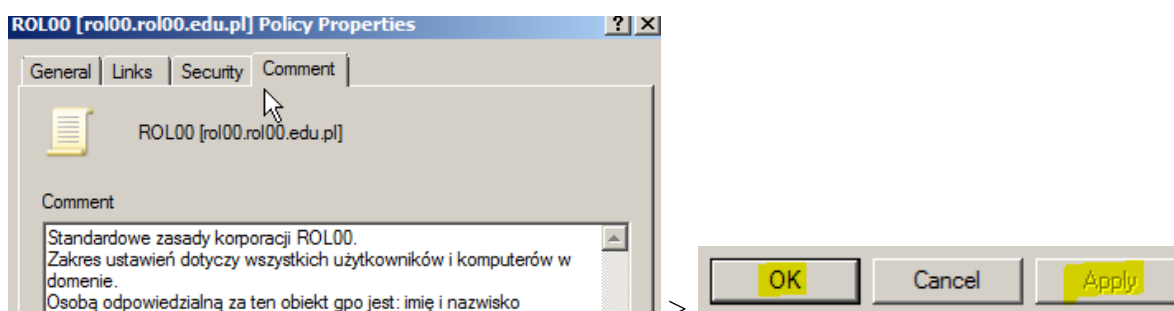
Kliknij prawym przyciskiem myszy ROL00 gdzie 00 jest numerem twojego stanowiska



Kliknij prawym przyciskiem myszy węzeł główny konsoli i wybierz Properties (Właściwości).

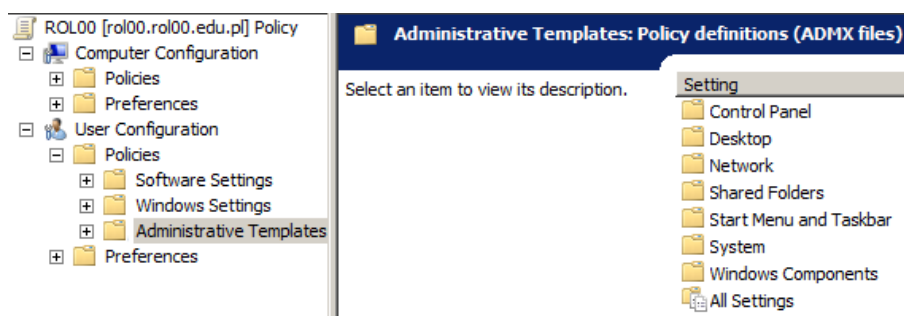


Kliknij zakładkę Comment (Komentarz) i wpisz jak poniżej



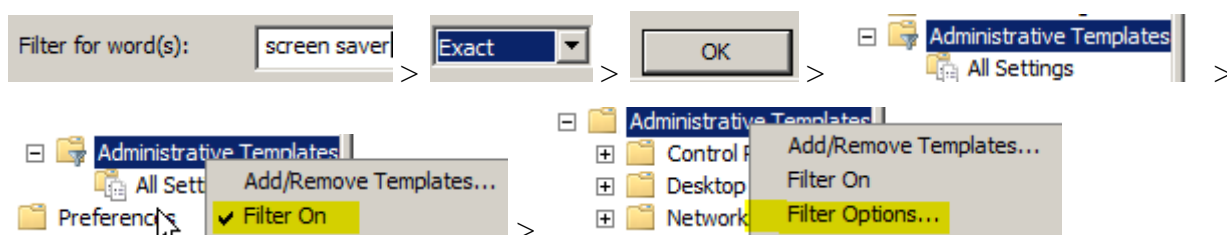
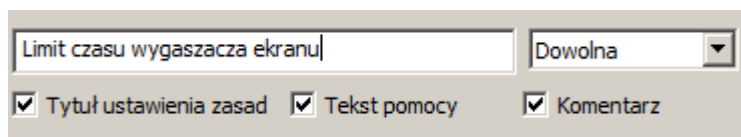
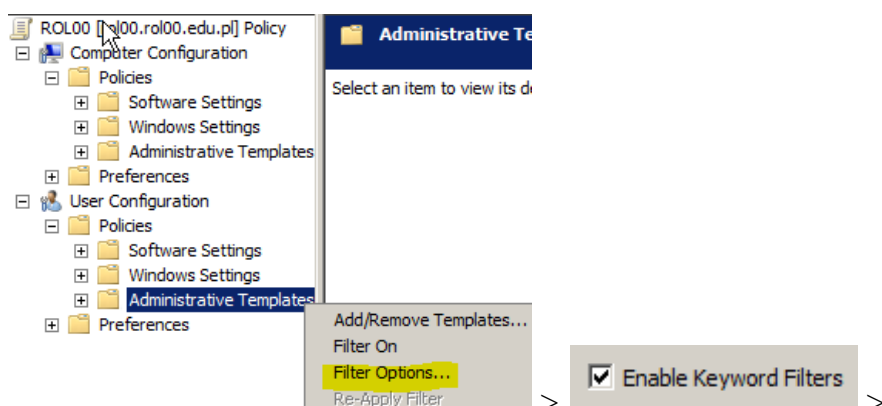
Skonfiguruj standardowe zasady korporacji które określają że komputery nie mogą być pozostawione bez opieki i w stanie zalogowania przez dłużej niż 10 minut, w tym celu:

Rozwiń węzeł User Configuration\Policies\Administrative Templates (Konfiguracja użytkownika \Zasady\Szablony administracyjne)



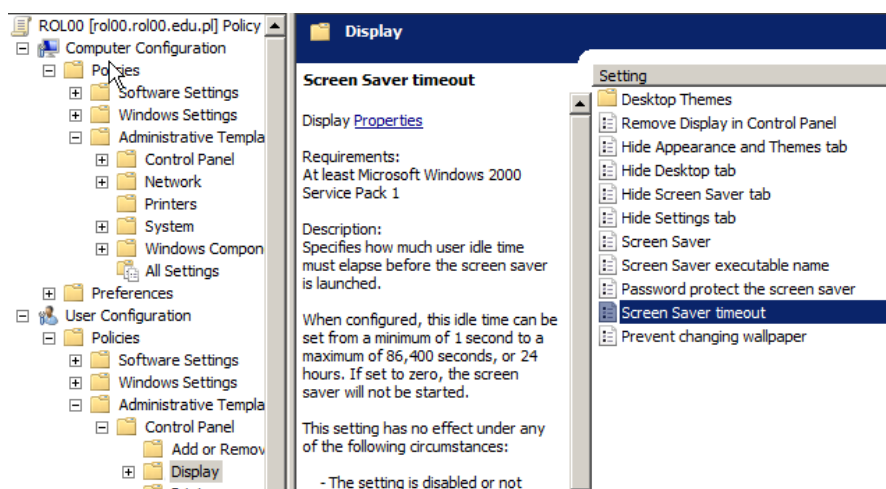
Przejrzyj ustawienia w tym węźle, zwróć szczególną uwagę na tekst wyjaśnień dla ustawień zasad, nie dokonuj żadnych zmian podczas tej czynności.

Kliknij prawym przyciskiem myszy Administrative Templates (Szablony administracyjne) w węźle User Configuration (Konfiguracja użytkownika) wybierz Filter Options (Opcje filtru).

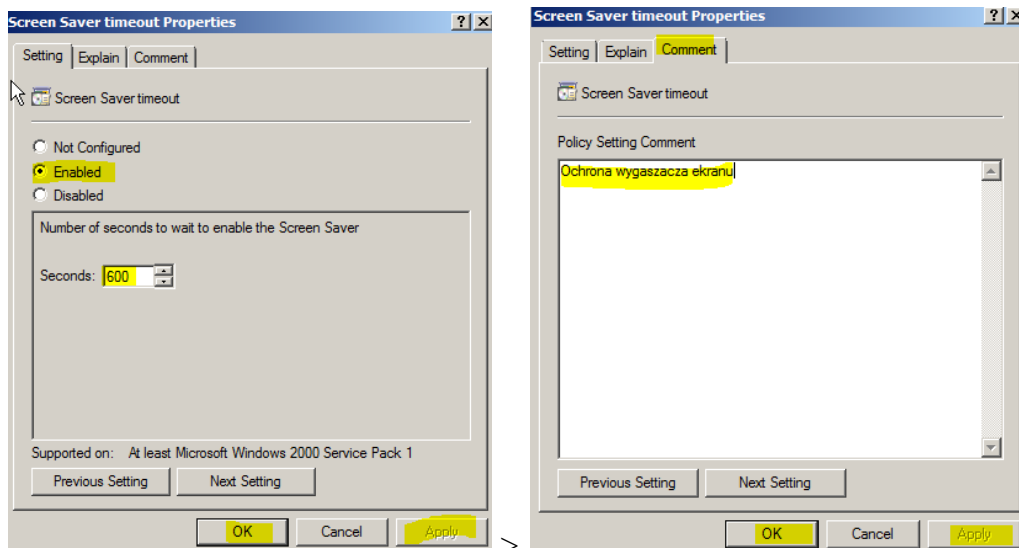


Ustawienia zasad w węźle Administrative Templates (Szablony administracyjne) zostaną przefiltrowane, pokazując tylko te, które zawierają słowa screen saver (wygaszacze).

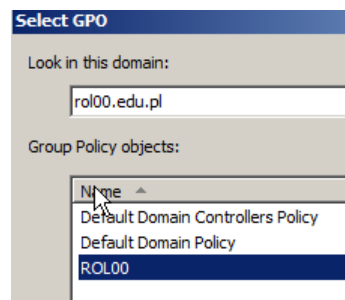
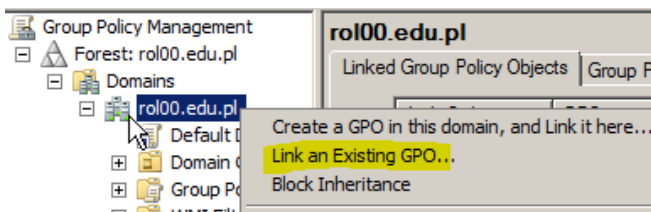
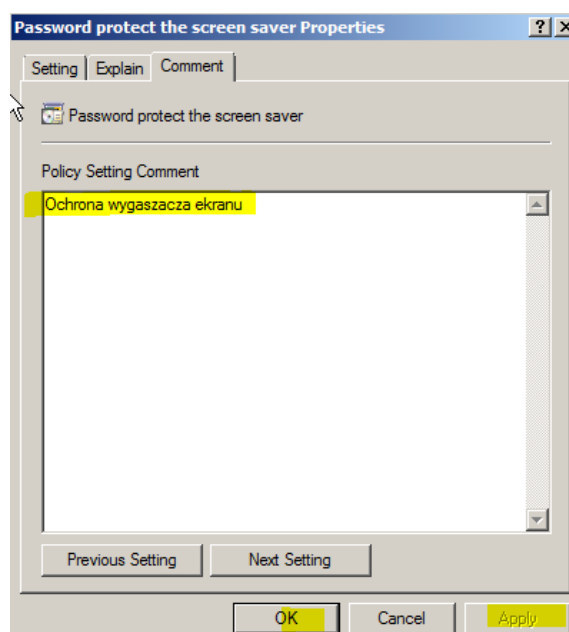
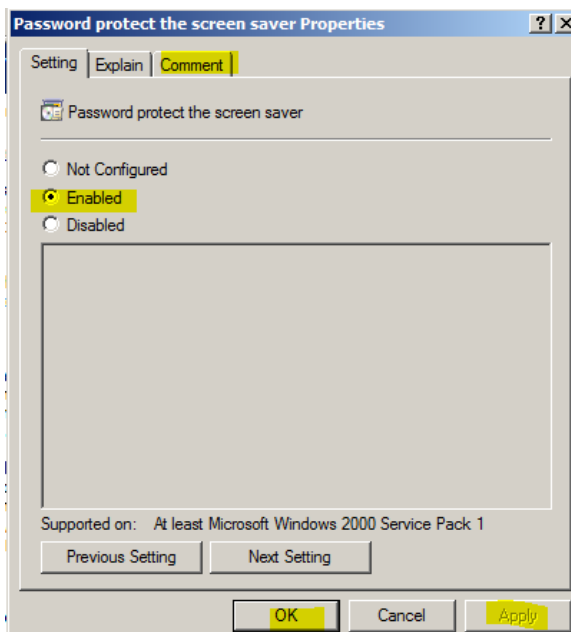
W węźle Control Panel\Display (Panel sterowania\Ekran) wybierz zasadę Screen Saver Timeout (Limit czasu wygaszacza ekranu), zwróć szczególną uwagę na tekst wyjaśnień.



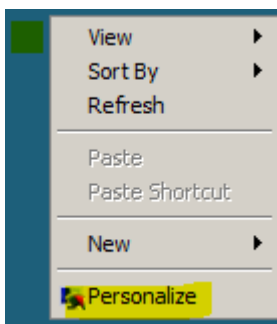
Podwójnie kliknij zasadę Screen Saver timeout (Limit czasu wygaszacza ekranu)



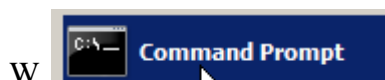
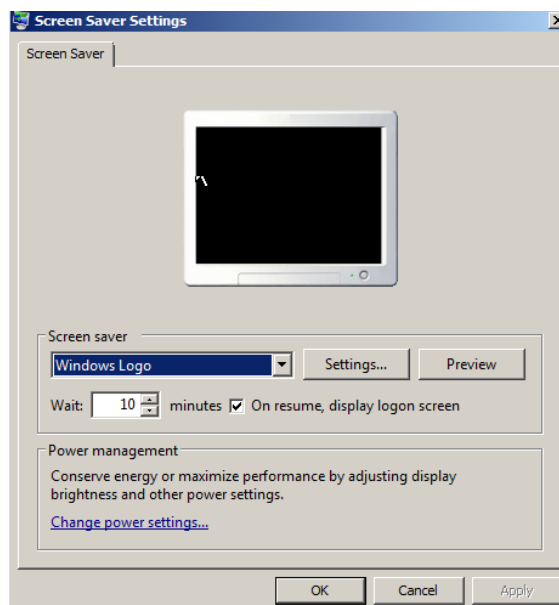
Podwójnie kliknij zasadę Password protect the screen saver (wygaszacz ekranu chroniony hasłem)



Na serwerze kliknij na pulpit ppm



Screen Saver
Change your screen and appearance

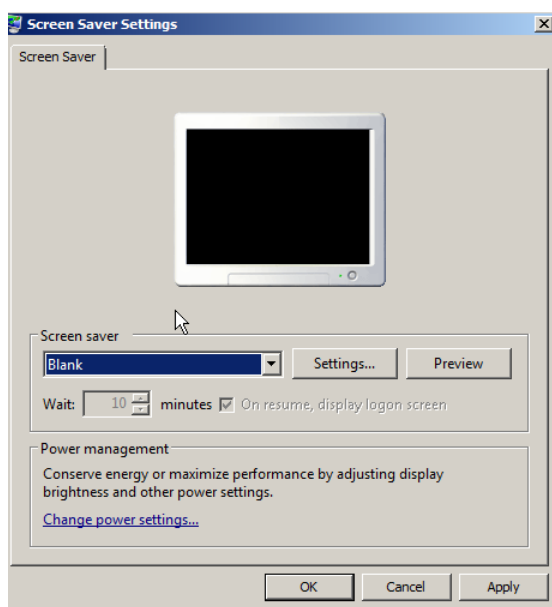


W wierszu polecenia wpisz

```
C:\Users\Administrator>gpupdate /force /boot /logoff
Updating Policy...
```

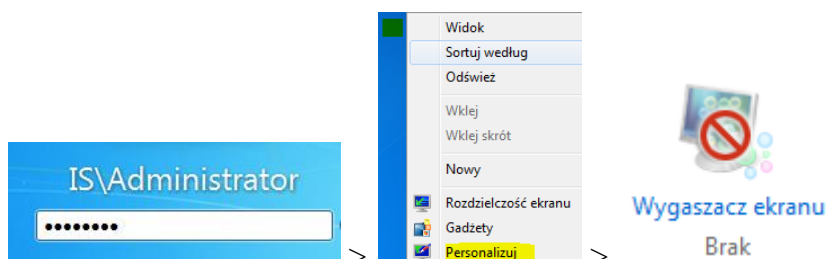
```
User Policy update has completed successfully.
Computer Policy update has completed successfully.
```

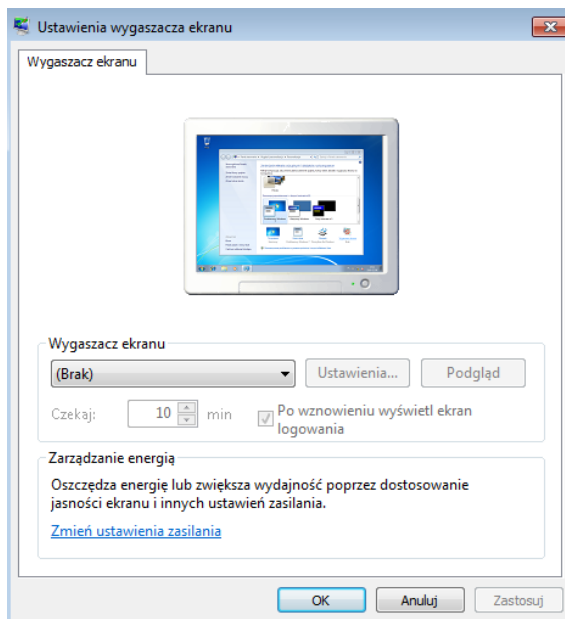
Te opcje polecenia *Gpupdate.exe* wywołują najpełniejsze odświeżenie zasad grupy. Należy poczekać aż zostaną zaktualizowane zarówno zasady użytkownika, jak i zasady komputera.



Zwróć uwagę, że po zastosowaniu zmiany zasad (odświeżeniu) nie można zmienić ustawień wygaszacza ekranu na serwerze.

Uruchom klienta (stację roboczą) Windows w wersji klienckiej (np. Windows 7), zaloguj się do konta Administrator.

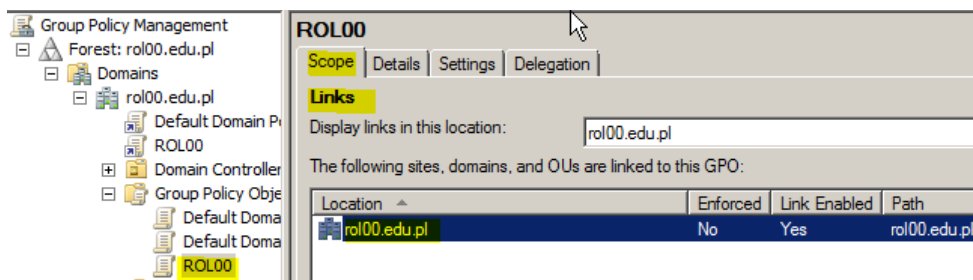




Zapisz notatkę, zwróć uwagę, że po zastosowaniu zmiany zasad (odświeżeniu) nie można zmienić ustawień wygaszacza ekranu na kliencie. Zasady obowiązują również na kliencie podłączonym do domeny.

Zadanie 2

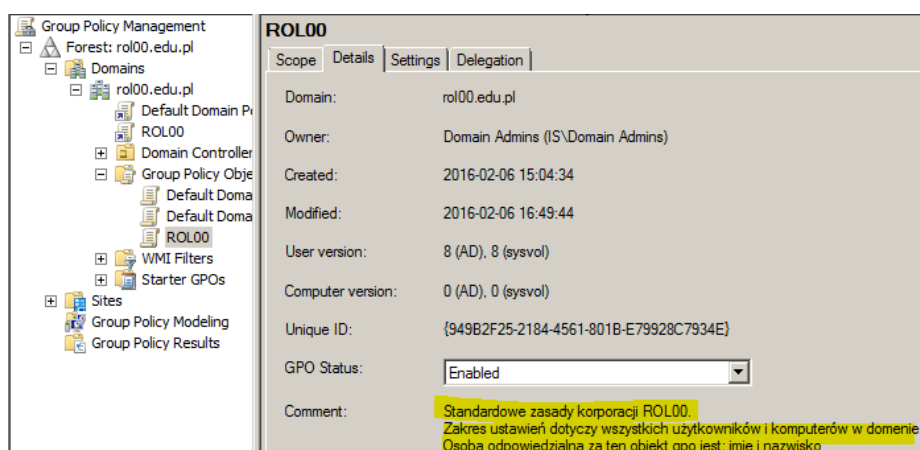
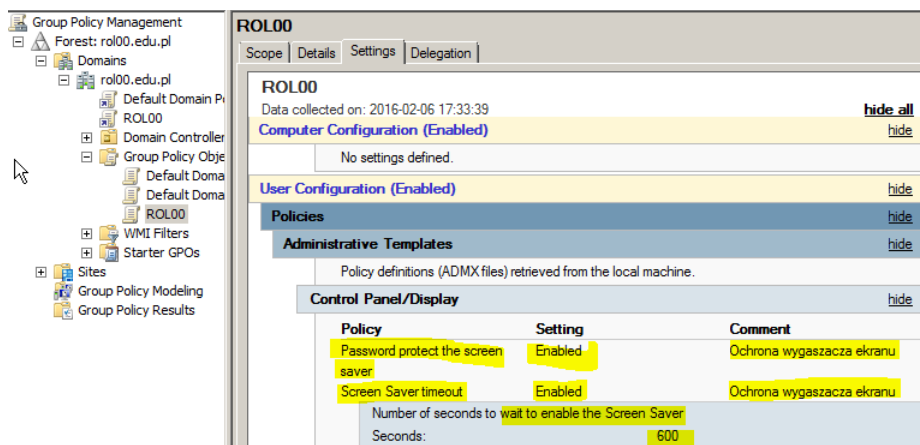
Badanie obiektu zasad grupy.



Kliknąć kartę Settings (Ustawienia), aby zobaczyć raport dotyczący ustawień zasad w tym obiekcie zasad grupy.

Jeśli mamy włączoną konfigurację zwiększonych zabezpieczeń programu Internet Explorer (ESC), to zostaniemy poproszeni o potwierdzenie, że chcemy dodać stronę `about:security_mmc.exe` do strefy Trusted Sites (Zaufane witryny).

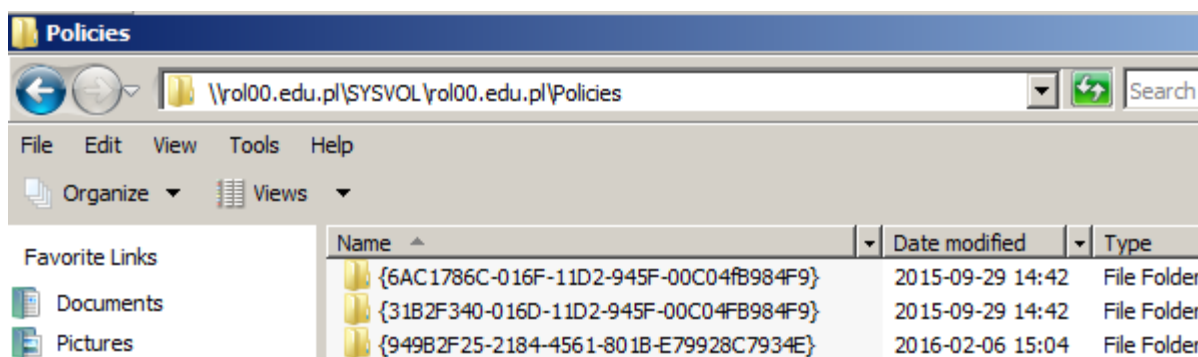
[show all](#)

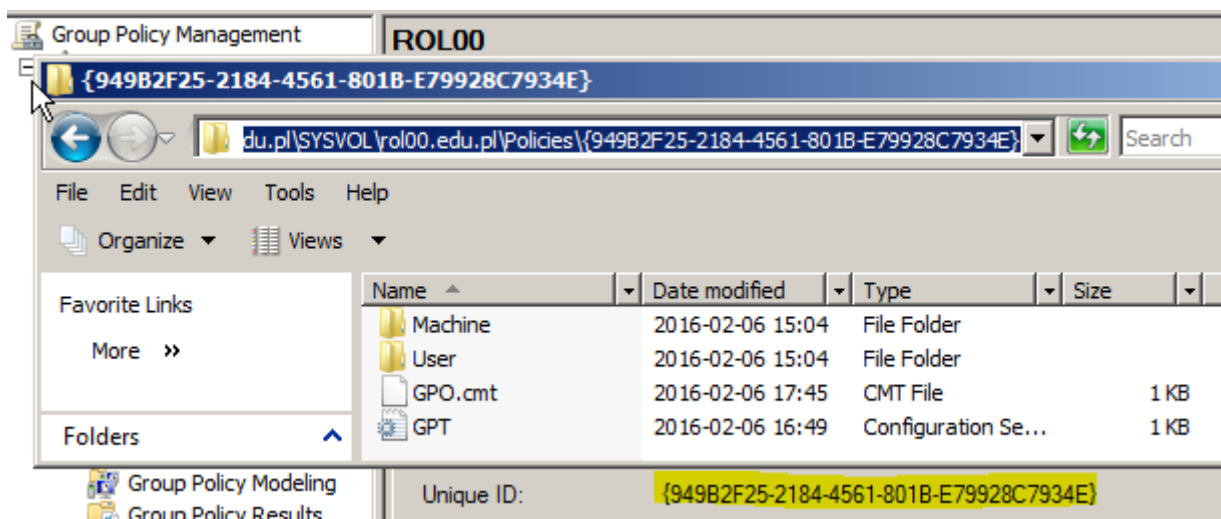


Zapisz unikatowy identyfikator obiektu pokazany na karcie Details (Szczegóły)

Np.: Unique ID: {949B2F25-2184-4561-801B-E79928C7934E}

Otwórz folder \\rol00.edu.pl\SYSVOL\rol00.edu.pl\Policies



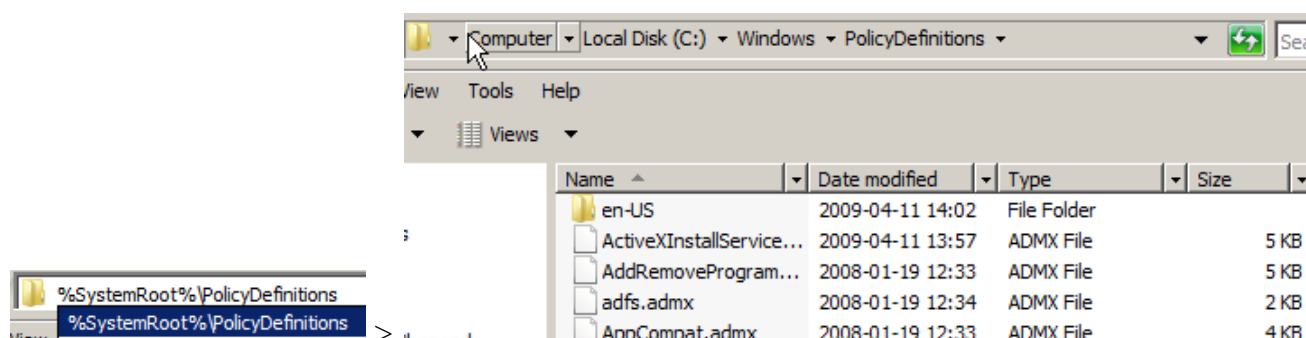


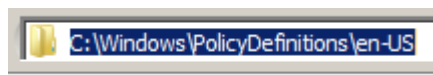
Jest to szablon GPT obiektu GPO.

Zadanie 3

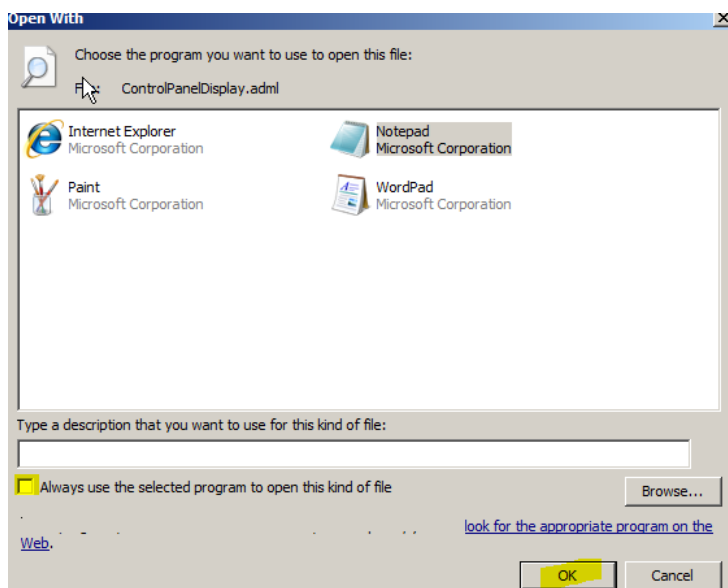
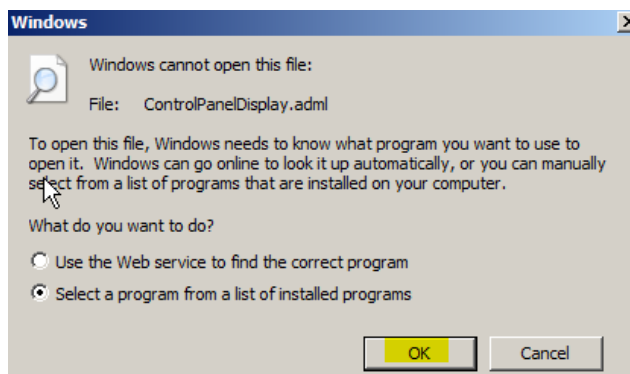
Badanie szablonów administracyjnych.

Szablony administracyjne zapewniają instrukcje, dzięki którym edytor zarządzania zasadami grupy tworzy interfejs użytkownika do konfigurowania ustawień zasad w węźle Administrative Templates (Szablony administracyjne) i określania zmian rejestru, które trzeba przeprowadzić w oparciu o te ustawienia zasad. W tym ćwiczeniu zbadamy szablon administracyjny.

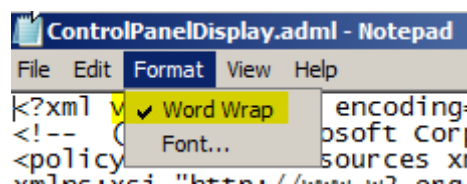




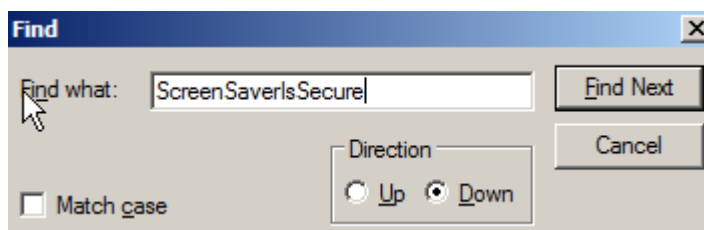
> pk >



>



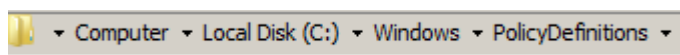
Wyszukaj tekst



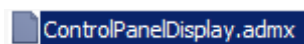
SeverIs > I to jest duża litera I jak Irek

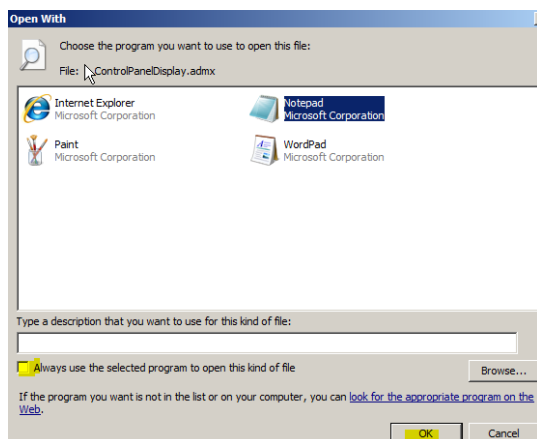
Zwróć uwagę na tekst wyjaśniający w następnym wierszu, zapisz w zeszytcie czego dotyczy.

Zamknij plik i przejdź do folderu jak poniżej

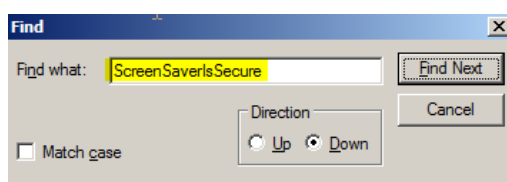


>





Wyszukaj tekst



```
<policy name="ScreenSaverIsSecure" class="user"
displayName="$(string.ScreenSaverIsSecure)"
explainText="$(string.ScreenSaverIsSecure_Help)"
key="Software\Policies\Microsoft\windows\Control Panel\Desktop"
valueName="ScreenSaverIsSecure">
  <parentCategory ref="Display" />
  <supportedOn ref="windows:SUPPORTED_win2kSP1" />
  <enabledvalue>
    <string>1</string>
  </enabledvalue>
  <disabledvalue>
    <string>0</string>
  </disabledvalue>
</policy>
```

Zidentyfikuj następujące elementy, zapisz je do zeszytu:

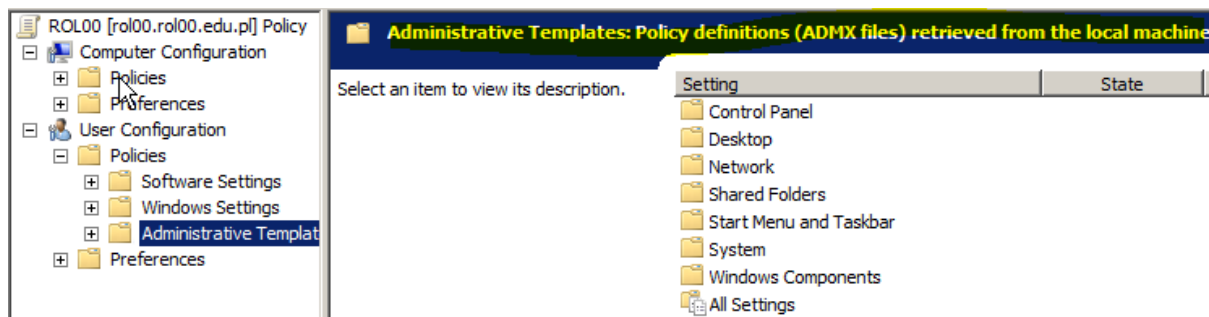
- Nazwę ustawienia zasad, która pojawia się w edytorze zarządzania zasadami grupy
- Tekst wyjaśniający dla ustawienia zasad
- Klucz rejestru i wartość modyfikowaną przez to ustawienie zasad
- Dane wstawione do rejestru, jeśli zasada jest włączona
- Dane wstawione do rejestru, jeśli zasada jest wyłączona

Zadanie 4

Tworzenie magazynu centralnego.

Utwórz magazyn centralny szablonów administracyjnych do scentralizowanego zarządzania szablonami.

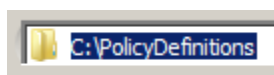
Rozwinąć węzeł User Configuration\Policies\Administrative Templates
(Konfiguracja użytkownika\Zasady\Szablony administracyjne).



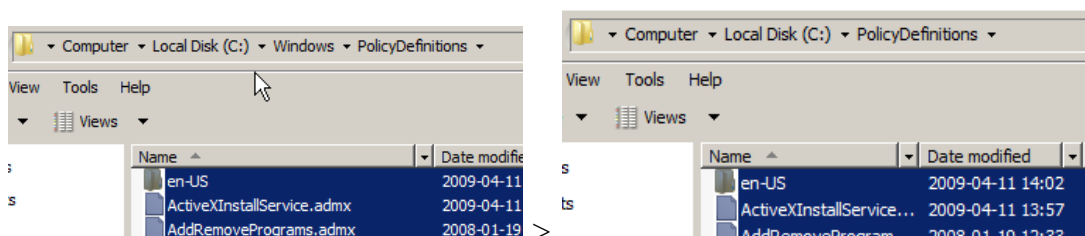
Węzeł Szablony administracyjne pobierany jest z komputera lokalnego.

Zamknij zarządzania zasadami grupy.

Utwórz folder o nazwie PolicyDefinitions.



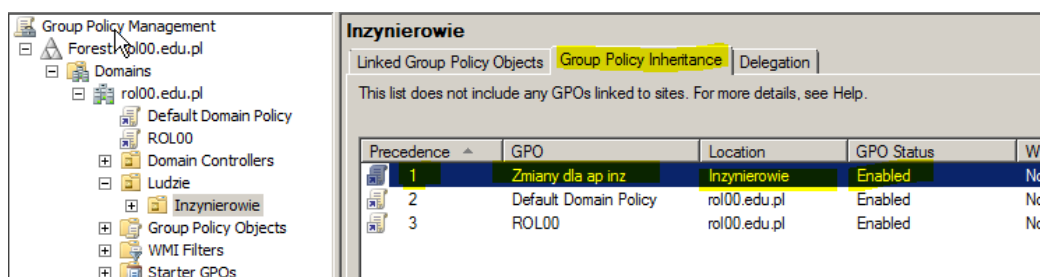
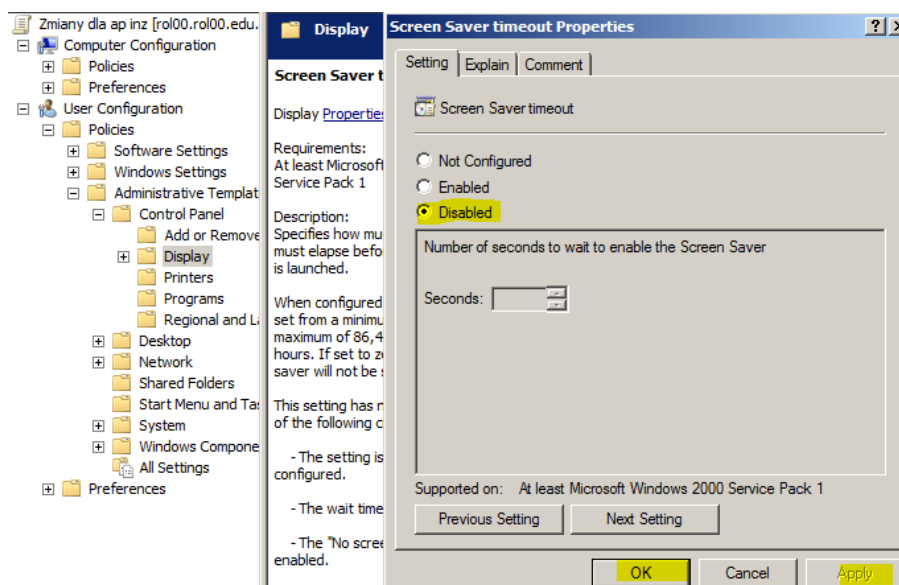
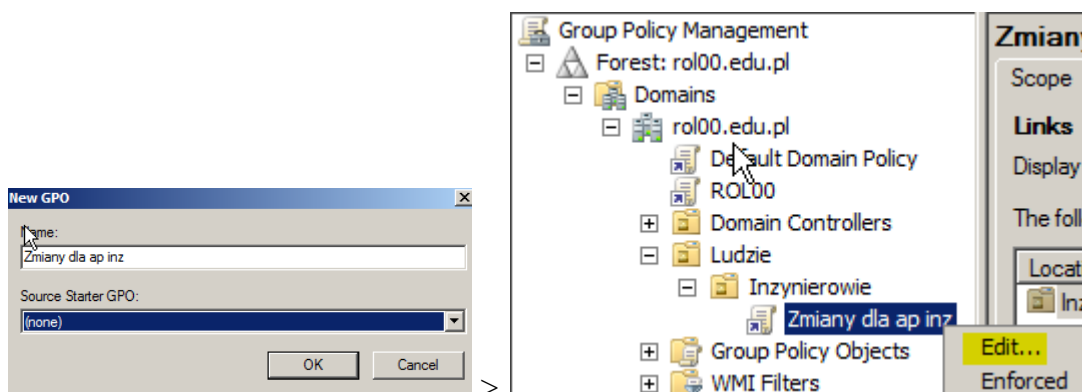
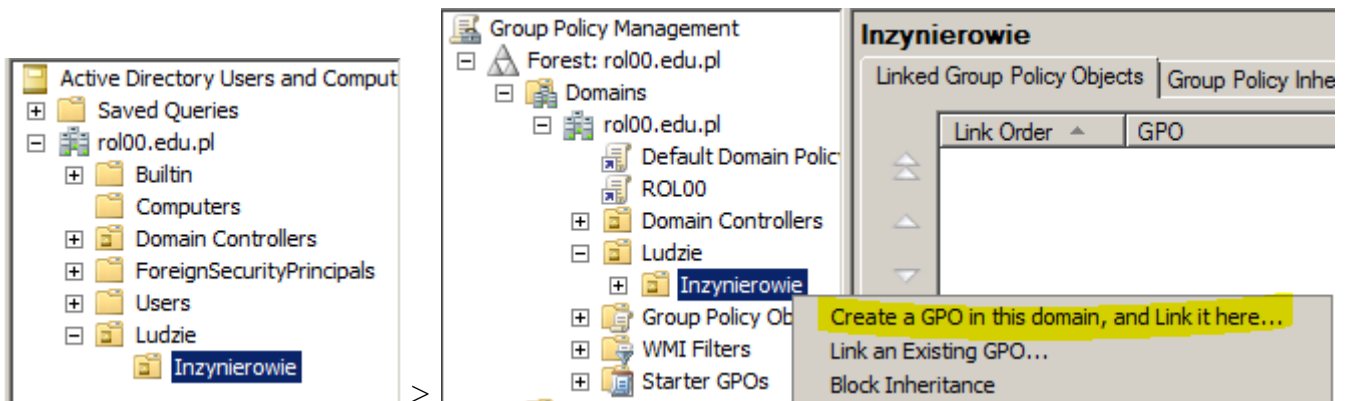
Skopiuj zawartość foldera %SystemRoot%\PolicyDefinitions do foldera utworzonego w poprzednim kroku.



Zadanie 5

Tworzenie obiektu GPO z ustawieniami zasad mającymi pierwszeństwo nad ustawieniami będącymi w konflikcie.

Obiekt zasad grupy ROL00, przyłączony do domeny, konfiguruje ustawienia zasad wymagające 10-minutowego okresu przed włączeniem się wygaszacza ekranu. Pewien inżynier zgłasza, że krytyczna aplikacja wykonująca długotrwałe obliczenia zawiesza się, gdy uruchomi się wygaszacz ekranu i prosi o niestosowanie tego ustawienie w przypadku zespołu inżynierów, korzystających z tej aplikacji.



Zwrócić uwagę, że obiekt zasad grupy **Zmiany dla ap inz** ma pierwszeństwo przed obiektem zasad grupy ROL00.

Skonfigurowane przez nas ustawienie, które jawnie wyłącza wygaszacz ekranu, uchyli ustawienie w obiekcie zasad grupy ROL00.

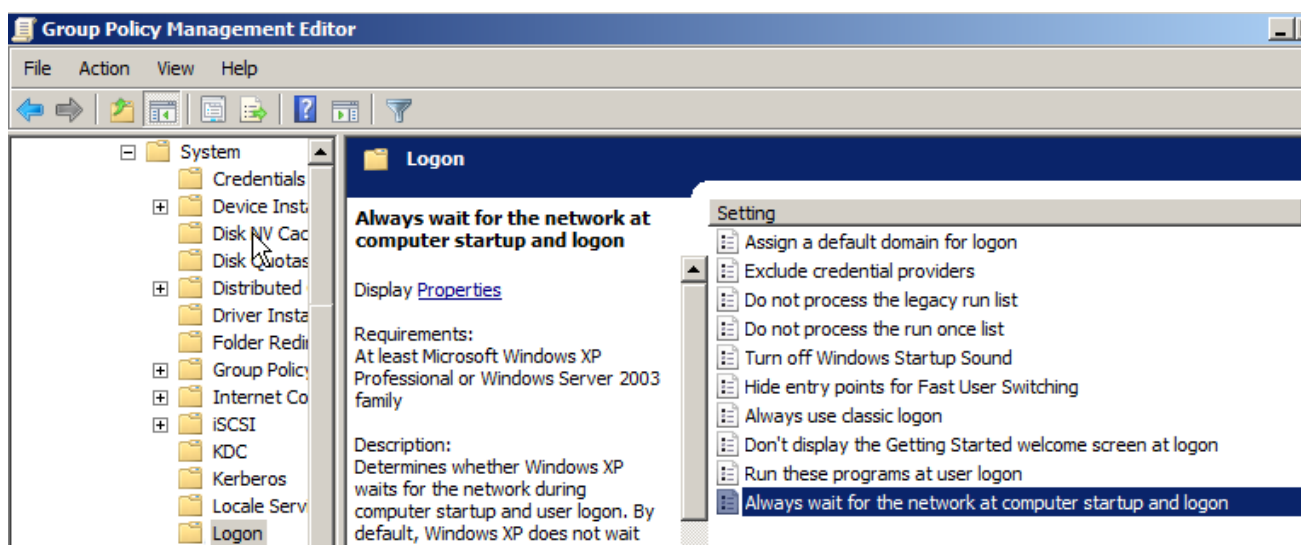
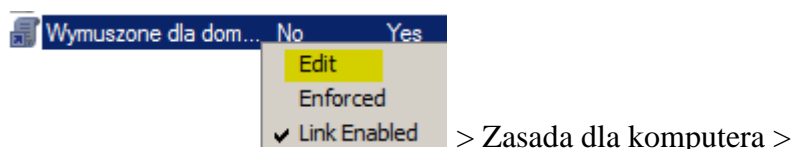
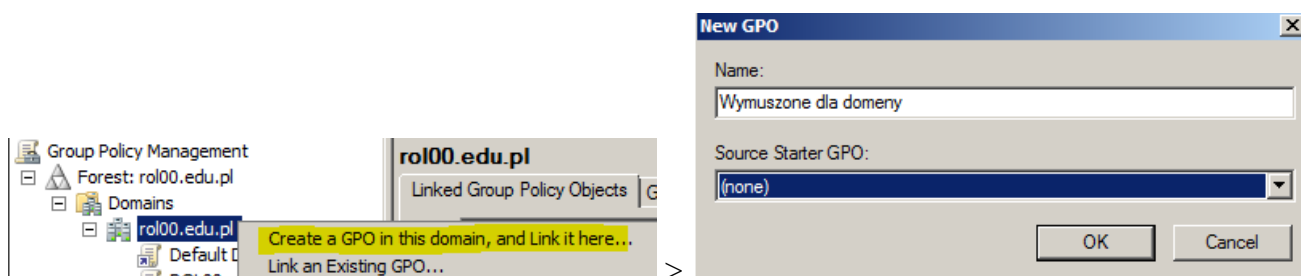
Obiekt **Zmiany dla ap inz** ma pierwszeństwo przed obiektem zasad grupy ROL00.

Zadanie 6

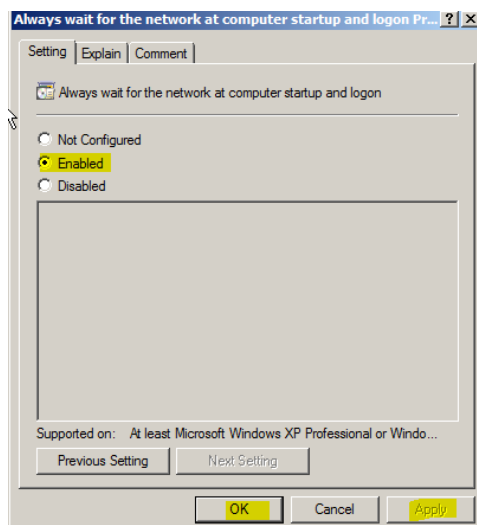
Konfigurowanie opcji Enforced (Wymuszenie)

Zapewnij, aby wszystkie systemy uzyskiwały zmiany zasad grupy tak szybko jak to możliwe.

W tym celu należy włączyć ustawienie zasad grupy Always Wait for The Network (Zawsze czekaj na sieć). Administratorzy nie mogą uchylać tego ustawienia, musi być ono wymuszane dla wszystkich systemów.

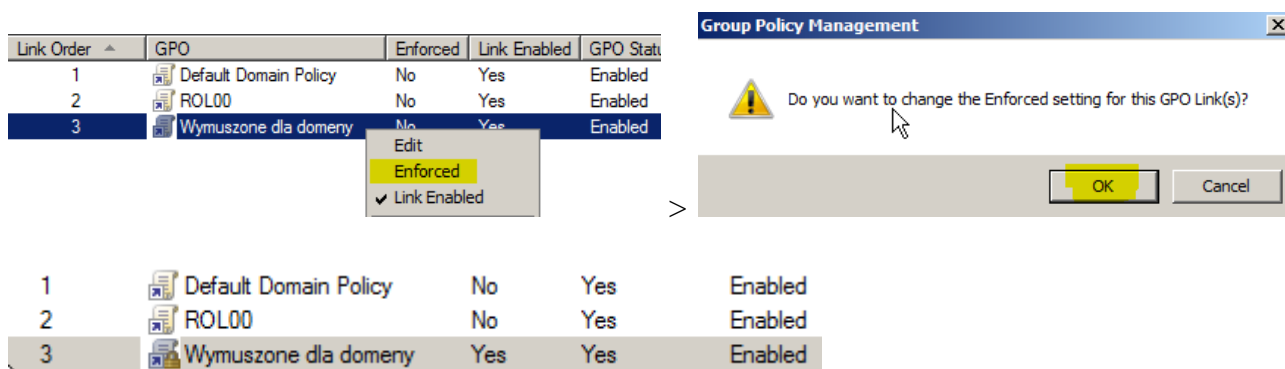


Podwójnie kliknij ustawienie zasad Always Wait for The Network At Computer Startup And Logon (Zawsze czekaj na sieć podczas uruchomienia komputera i logowania).



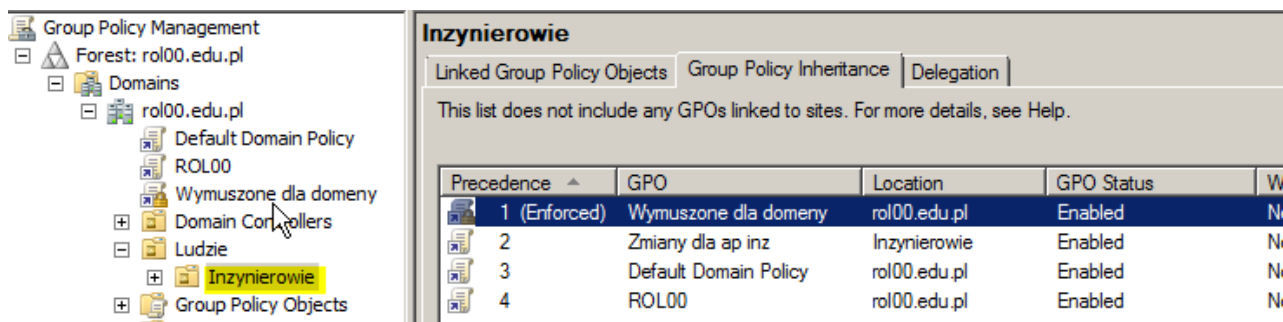
Zamknąć Edytor zarządzania zasadami grupy.

Kliknąć prawym przyciskiem myszy obiekt zasad grupy Wymuszone zasady domenowe i wybrać Enforced (Wymuszone).



Zaznaczyć jednostkę organizacyjną Inżynierowie, a następnie kliknąć kartę Group Policy Inheritance (Dziedziczenie zasad grupy).

Zaznaczyć jednostkę organizacyjną Inżynierowie, a następnie kliknąć kartę Group Policy Inheritance (Dziedziczenie zasad grupy).

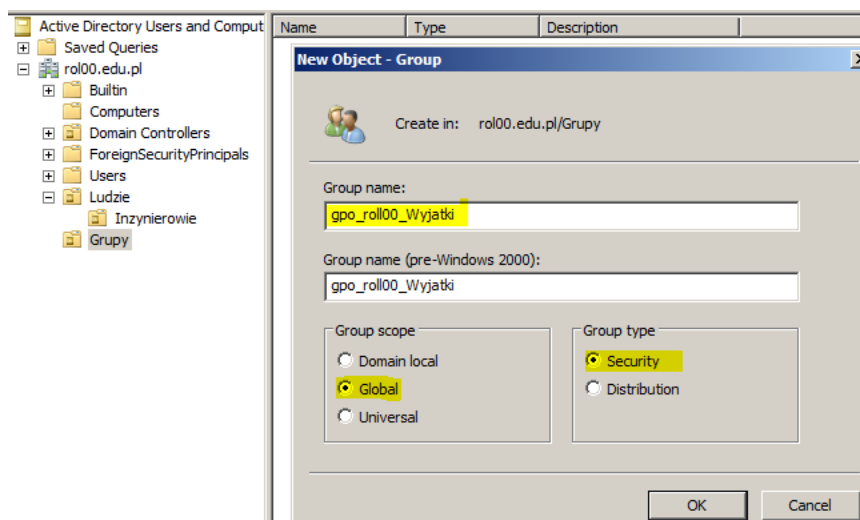


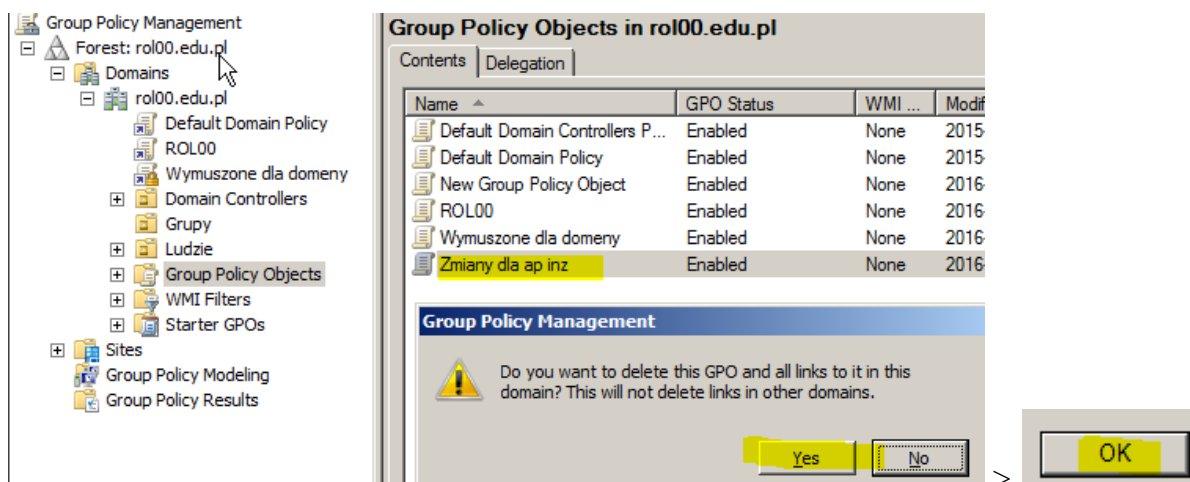
Należy zwrócić uwagę, że wymuszony, domenowy obiekt zasad grupy ma pierwszeństwo nawet przed obiektami zasad grupy przyłączonymi do jednostki organizacyjnej Inżynierowie. Ustawienia w obiekcie zasad grupy, takim jak **Zmiany dla ap inz** nie mogą uchylić ustawień w wymuszonym obiekcie zasad grupy.

Zadanie 7

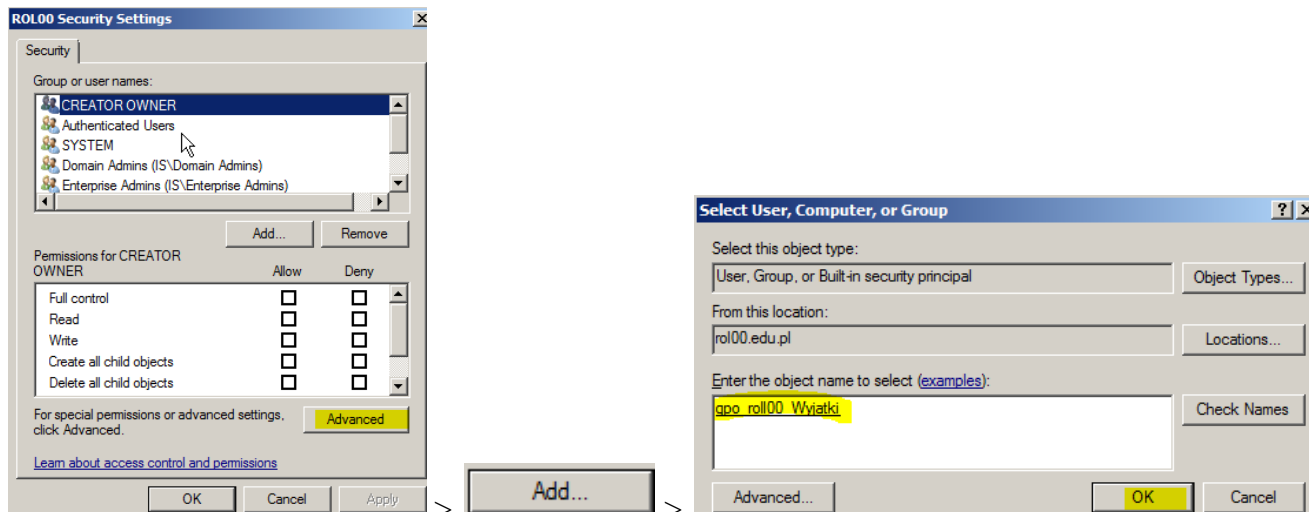
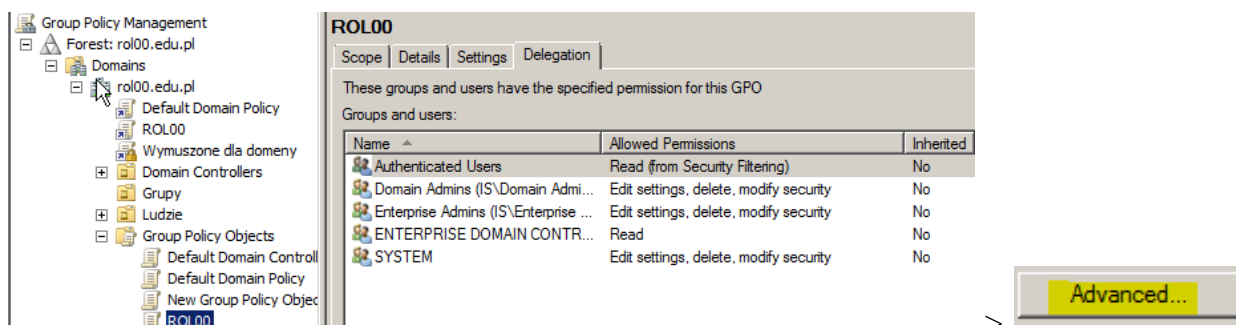
Konfigurowanie filtrowania zabezpieczeń.

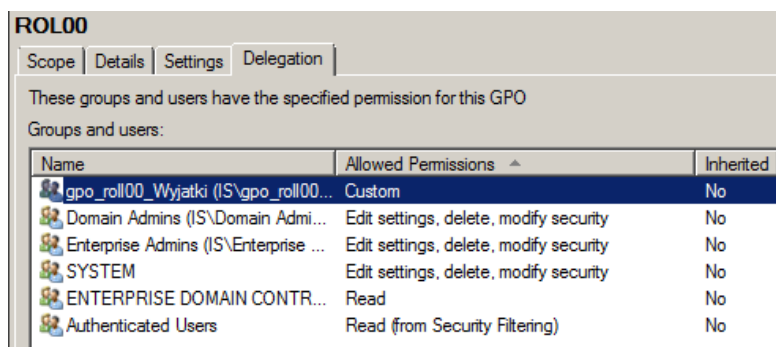
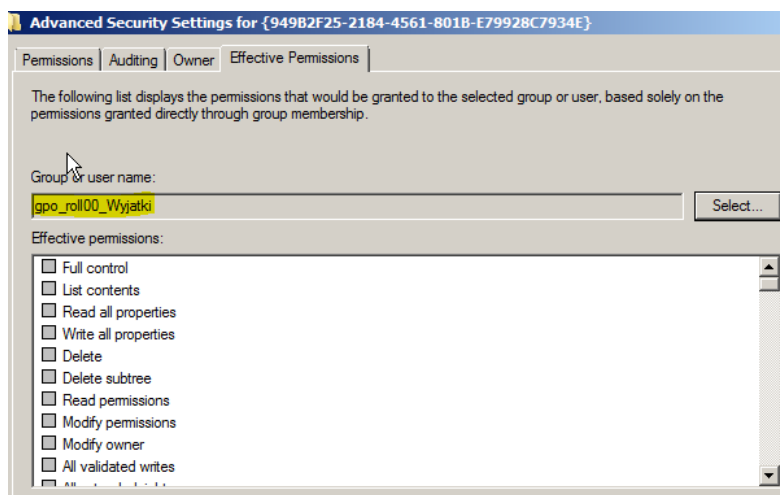
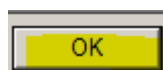
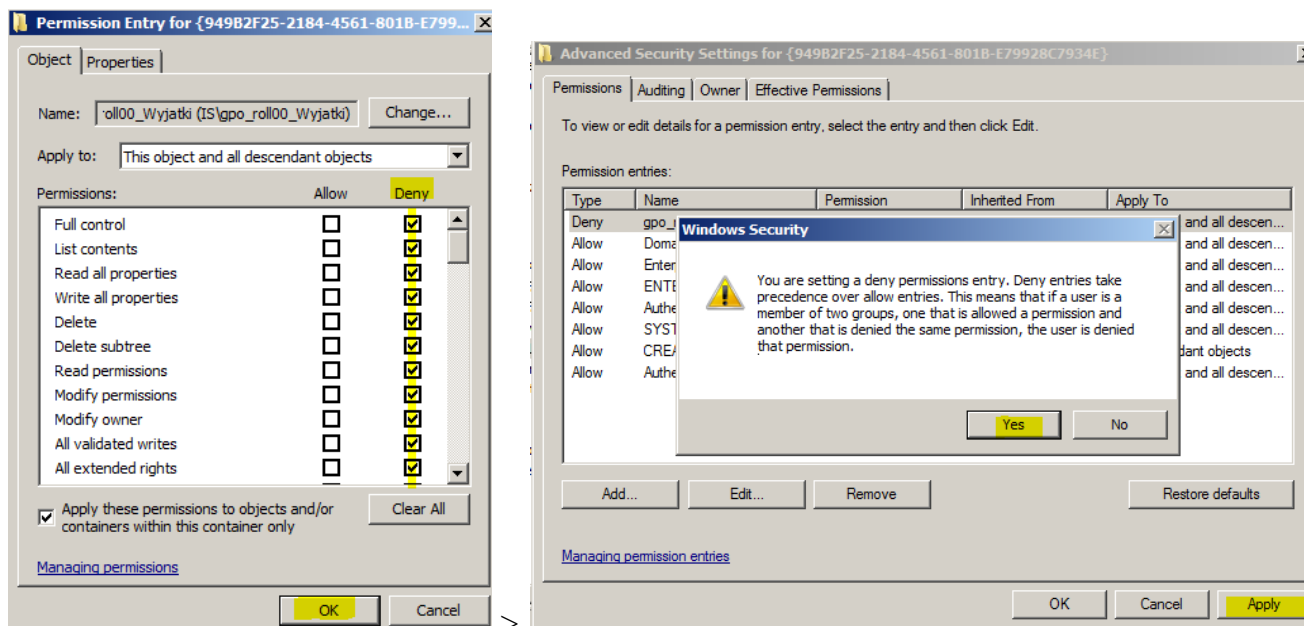
Odkrywamy, że niewielka liczba użytkowników musi być wyłączona z zasady ustalającej limit czasu dla wygaszacza ekranu, skonfigurowanej przez obiekt zasad grupy **ROL00**. Nie praktyczne było by uchylenie ustawień. Zastosuj filtrowanie zabezpieczeń w celu zarządzania zakresem obiektu zasad grupy.



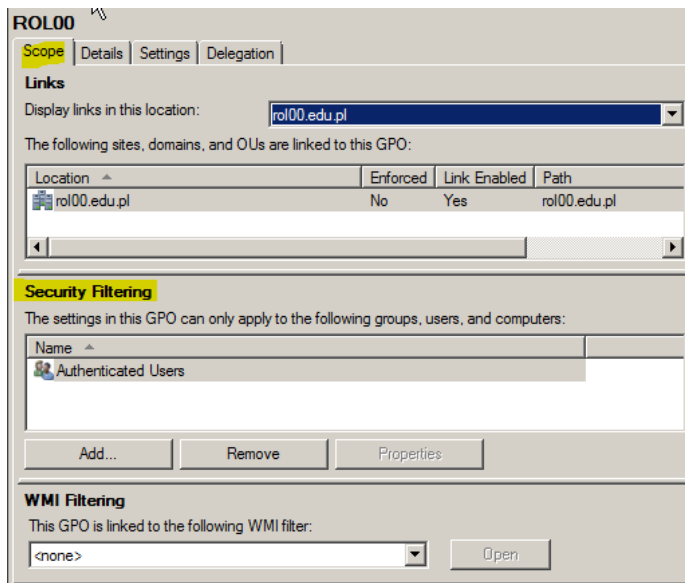


Zaznacz obiekt zasad grupy **ROL00** w kontenerze Group Policy Objects (Obiekty zasad grupy)





Kliknij kartę Scope (Zakres) i zbadaj sekcję Security Filtering (Filtrowanie zabezpieczeń).



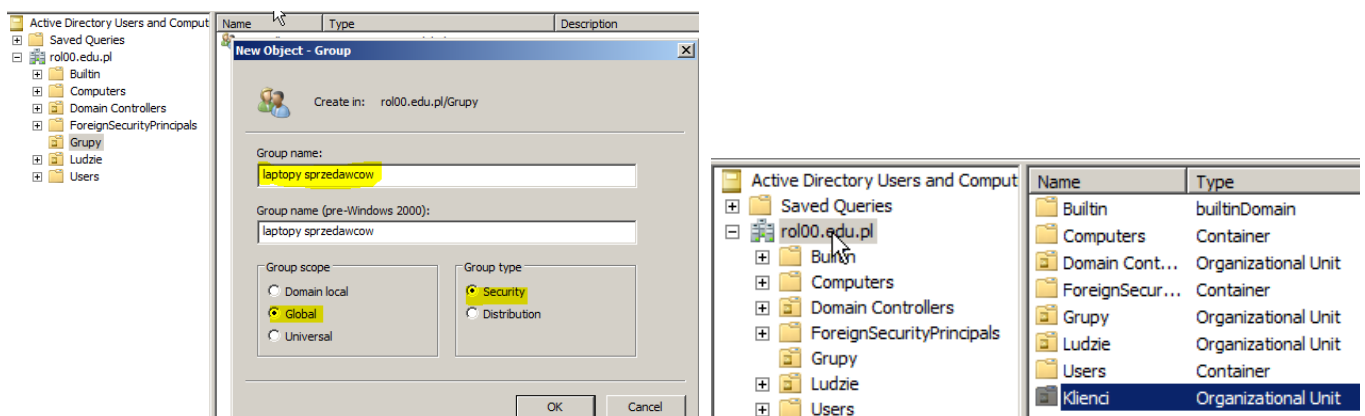
Domyślne filtrowanie zabezpieczeń dla nowego obiektu zasad grupy jest takie, że grupa Authenticated Users (Użytkownicy uwierzytelnieni) ma uprawnienie Allow Apply Group Policy (Zezwalaj Stosowanie zasad grup), więc wszyscy użytkownicy i komputery w zakresie tego łącza do obiektu GPO będą stosować ustawienia w tym obiekcie GPO. Skonfigurowaliśmy grupę z uprawnieniem Deny Apply Group Policy (Odmów Stosowanie zasad grup), które uchyla uprawnienie Allow (Zezwalaj). Jeśli jakiś użytkownik wymaga wyłączenia z zasad w obiekcie zasad **ROL00** to można dodać go do tej grupy.

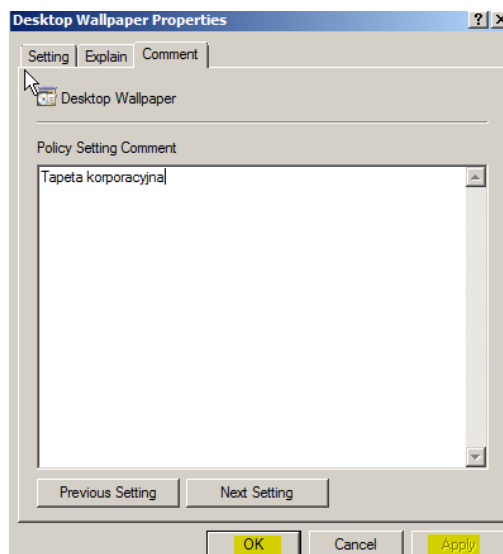
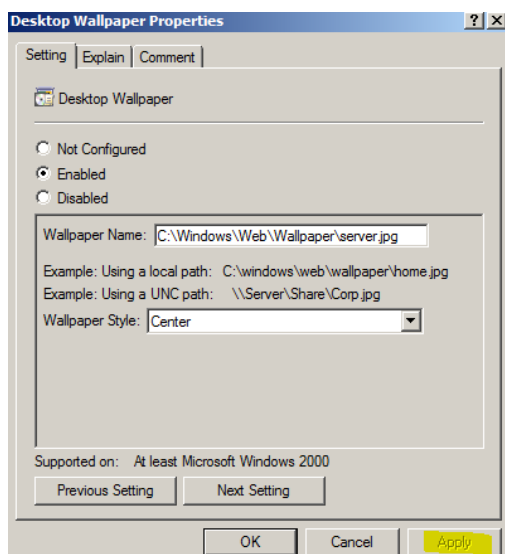
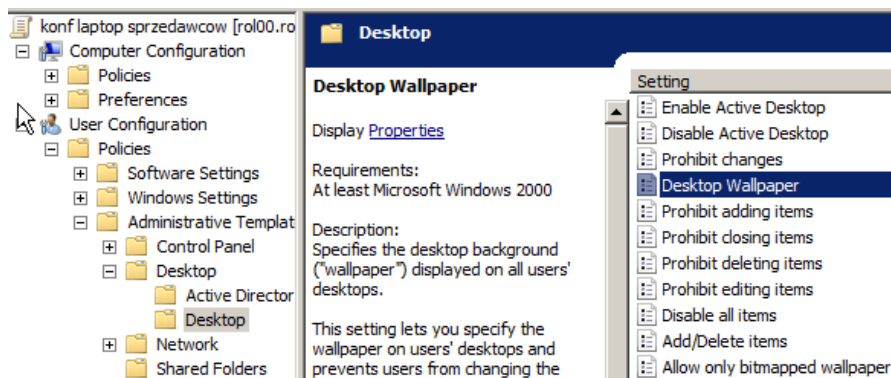
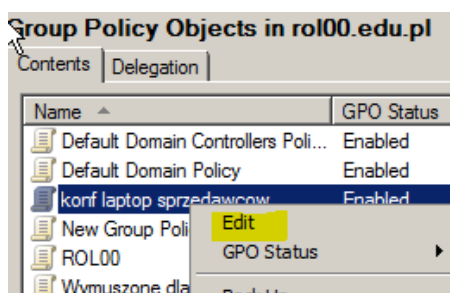
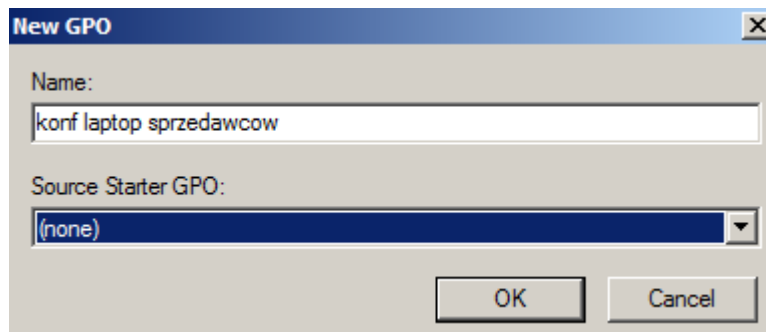
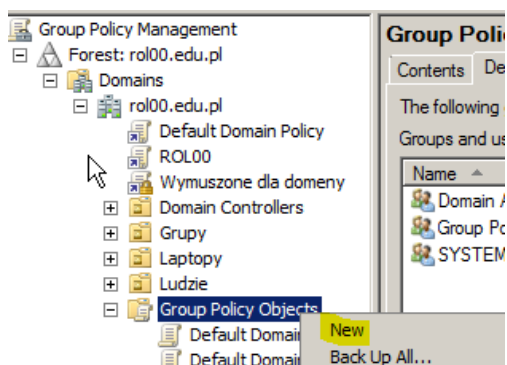
Zapisz w zeszycie na czym polega filtrowanie zabezpieczeń.

Zadanie 8

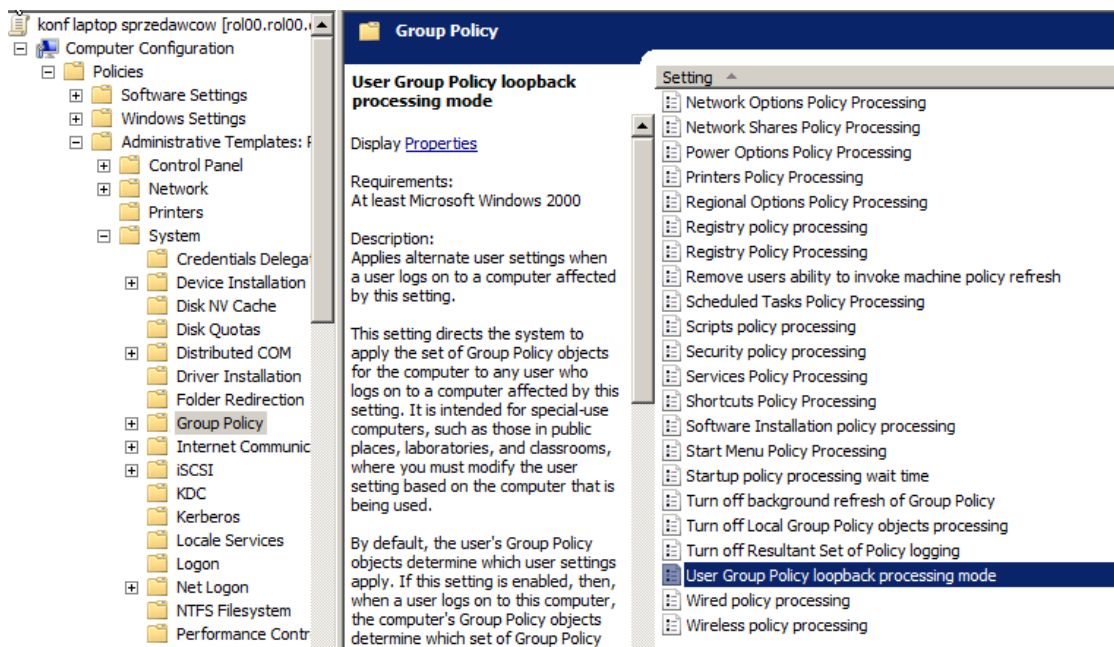
Przetwarzanie zasad w sprzężeniu zwrotnym.

Sprzedawca w firmie **ROL00** włączył swój komputer, aby przeprowadzić prezentację dla ważnego klienta, a na tapecie pulpitu był obraz, który świadczył o wątpliwym guście tego sprzedawcy. Zarząd poprosił o zapewnienie, żeby laptopy używane przez sprzedawców, gdy są oni zalogowani nie miały tapety, nie jest to konieczne, gdy są oni zalogowani do kont na komputerach w biurze. Obiekty komputerów dla laptopów są rozproszone po kilku jednostkach organizacyjnych, więc należy użyć filtrowania zabezpieczeń.

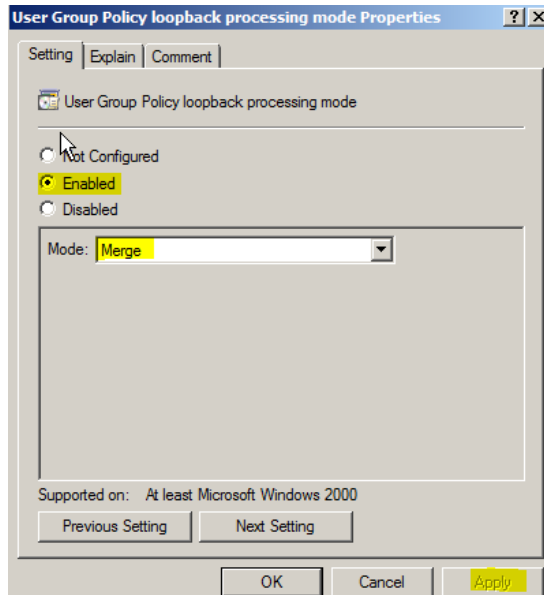




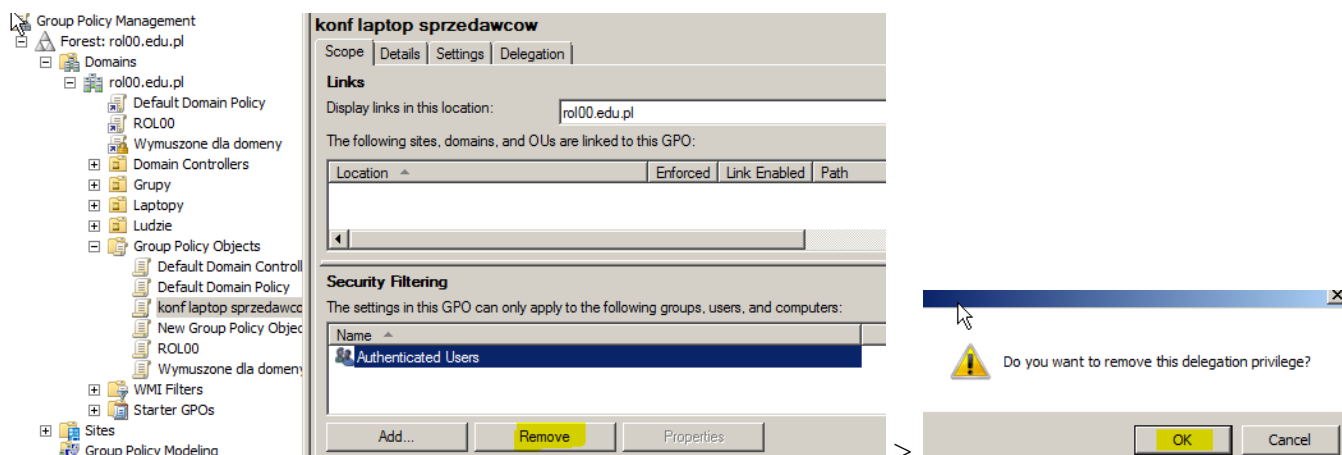
Rozwinąć węzeł Computer Configuration\Policies\Administrative Templates\System\Group Policy (Konfiguracja komputera\Zasady\Szablony administracyjne\System\Zasady grupy).
Podwójnie kliknąć ustawienie zasad User Group Policy Loopback Processing Mode (Tryb przetwarzania sprzężenia zwrotnego zasad grupy użytkownika).



Kliknąć Enabled (Włączone), a z listy rozwijanej Mode (Tryb) wybrać Merge (Scal).

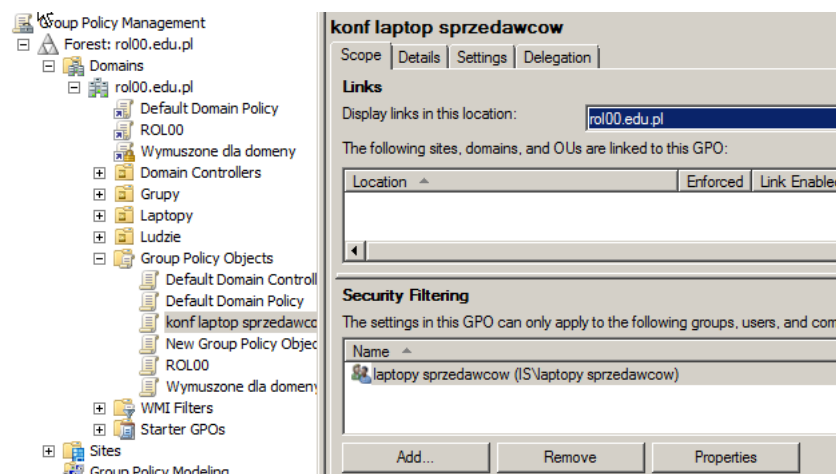
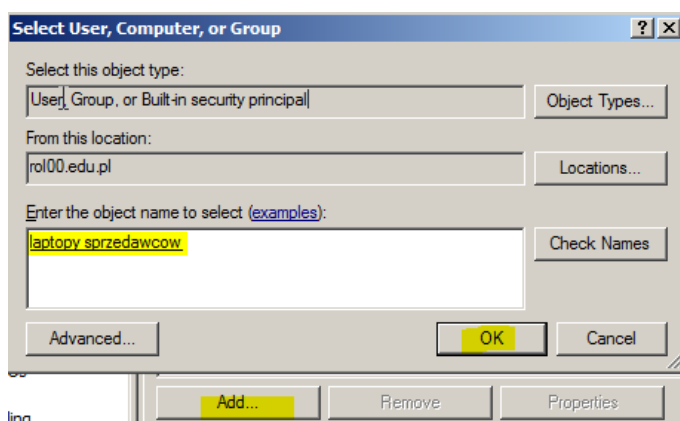


W konsoli Group Policy Management (Zarządzanie zasadami grupy) należy zaznaczyć obiekt zasad grupy Konfiguracja laptopów sprzedawców w kontenerze Group Policy Objects (Obiekty zasad grupy). Na karcie Scope (Zakres) w sekcji Security Filtering (Filtrowanie zabezpieczeń) należy zaznaczyć grupę Authenticated Users (Użytkownicy uwierzytelnieni) i kliknąć Remove (Usuń), Należy kliknąć OK. aby potwierdzić swój wybór.

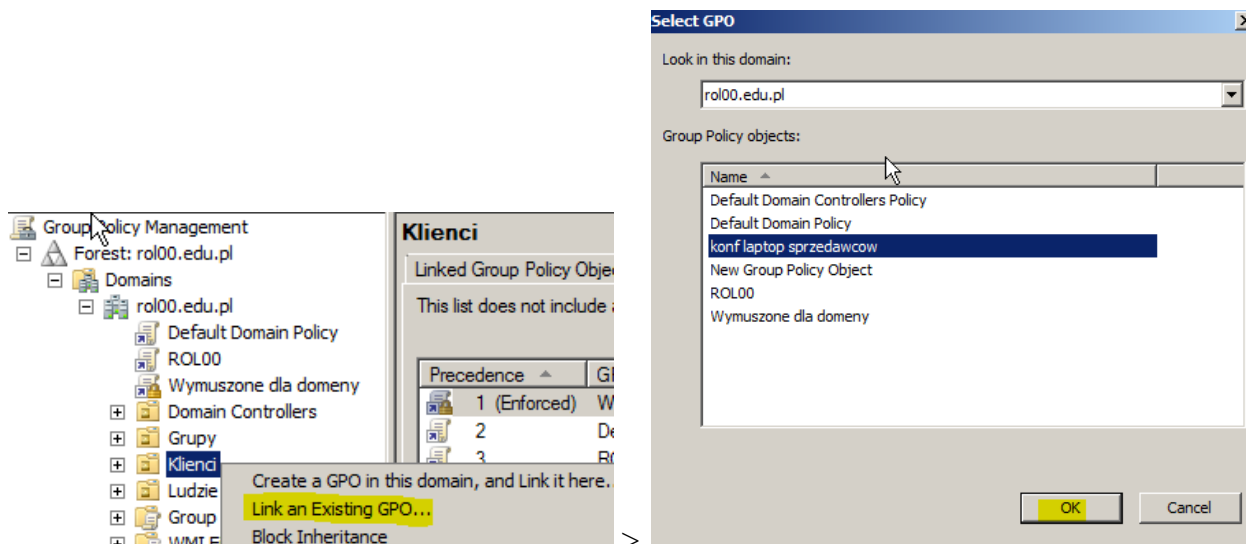


Kliknąć przycisk Add (Dodaj) W sekcji Security Filtering (Filtrowanie zabezpieczeń).

Wpisać nazwę grupy **laptopy sprzedawcow** i kliknąć OK.



Kliknąć prawym przyciskiem myszy jednostkę organizacyjną Klienci i wybrać opcję Link An Existing GPO (Połącz z istniejącym obiektem zasad grupy).



Ustawiliśmy filtrowanie obiektu zasad grupy tak, aby miał zastosowanie jedynie wobec obiektów w grupie Laptopy sprzedawców. Możemy dodać obiekty komputerów dla laptopów sprzedawców jako członków tej grupy, a te laptopy znajdą się w zakresie tego obiektu zasad grupy. Ten obiekt GPO konfiguruje laptopy tak, aby wykonywały przetwarzanie zasad w sprzężeniu zwrotnym w trybie Merge (Scal). Gdy użytkownik zaloguje się na jednym z tych laptopów, to ustawienia konfiguracji użytkownika obejmujące zakresem tego użytkownika zostaną zastosowane, a następnie będą zastosowane ustawienia konfiguracji użytkownika w obiektach zasad grupy obejmujących zakresem komputer, w tym obiekt zasad grupy **Konf laptop sprzedawcow**.

Zapisz w zeszycie na czym polega przetwarzanie zasad w sprzężeniu zwrotnym.

Skróty

ppm – prawy przycisk myszy