12.3 Konfigurowanie zakresu zasad grup, obsługa zasad grup.

Cel ogólny lekcji: Nauczyć się konfigurować zakres zasad grup oraz obsługiwać zasady grup w systemie Windows.

Cele szczegółowe:

1. Poznanie procedury tworzenia, edycji i definiowania zakresu obiektu zasad grup.
2. Utrwalenie umiejętności zarządzania jednostkami organizacyjnymi i zasadami GPO poprzez ograniczenie dostępu do zasobów systemowych dla użytkowników tymczasowych.
3. Zastosowanie zasad grupy (GPO) do ograniczenia dostępu do przeglądarek internetowych dla wybranych użytkowników w środowisku domenowym z interfejsem systemu Windows.
4. Zrozumienie, jak działa konfiguracja standardowych zasad korporacji i jak można je dostosować do własnych potrzeb.
5. Nauczenie się badania obiektów zasad grupy i szablonów administracyjnych.
6. Praktyczne wykorzystanie wiedzy w konfiguracji zakresu zasad grup i testowaniu ich działania na przykładzie ustawień wygaszacza ekranu na serwerze i stacji roboczej.
7. Zrozumienie, jakie zmiany w zasadach grup obowiązują na serwerze i kliencie po odświeżeniu ustawień.

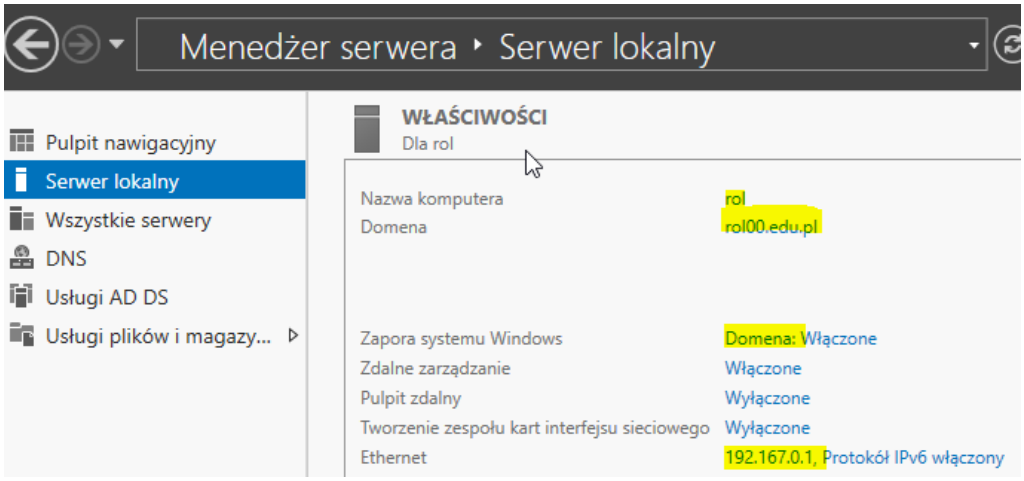
Przed przystąpieniem do ćwiczenia sprawdź i ustaw
W Menedżer funkcji Hyper-V wybierz nazwa maszynę wirtualna twojej grupy_dc2019

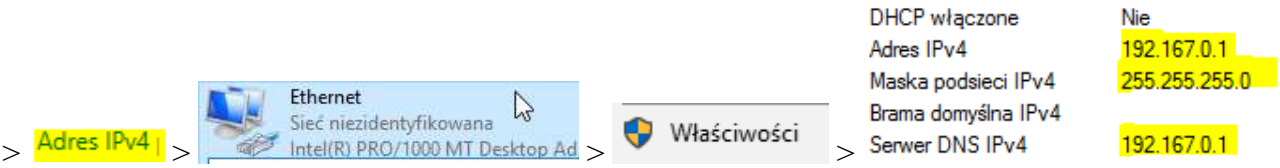
Upewnij się, że punk kontrolny, zawiera serwer z zainstalowanym kontrolerem domeny.

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

Przed przystąpieniem do ćwiczenia sprawdź i ustaw, jeśli to konieczne

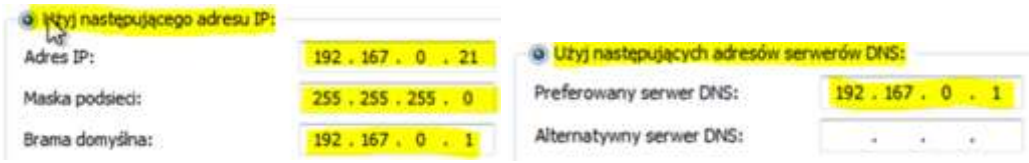
a) system serwera są jak poniżej:





Jeśli pracujesz w VirtualBox utwórz migawkę stanu systemu serwera o nazwie DDMM_numer

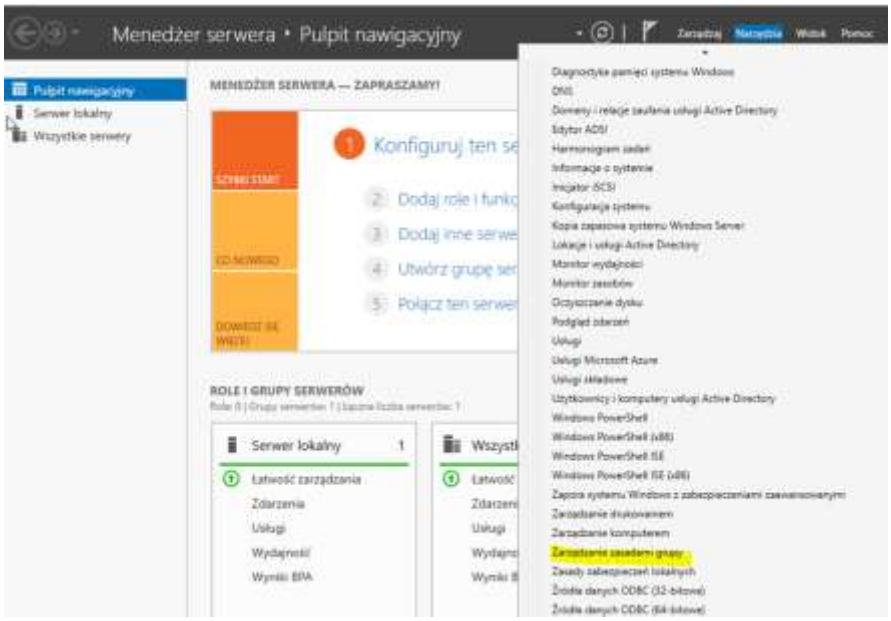
b) systemu klienta są jak poniżej:



W zeszycie opisz procedury tworzenie zasad grup w domenie.

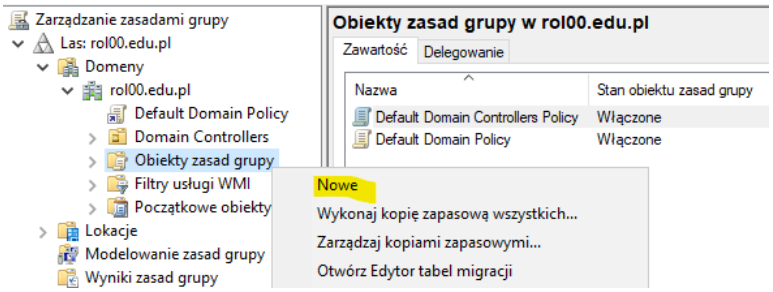
Zadanie 1a – Konfiguracja wygaszacza ekranu (Screen Saver Timeout)

Procedura tworzenia, edycji i definiowania zakresu obiektu zasad grup.

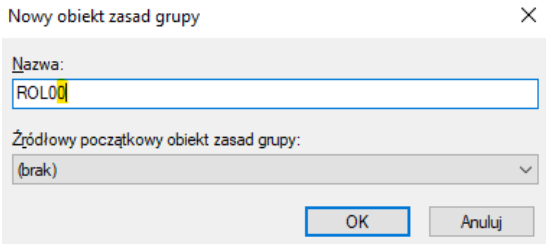


>

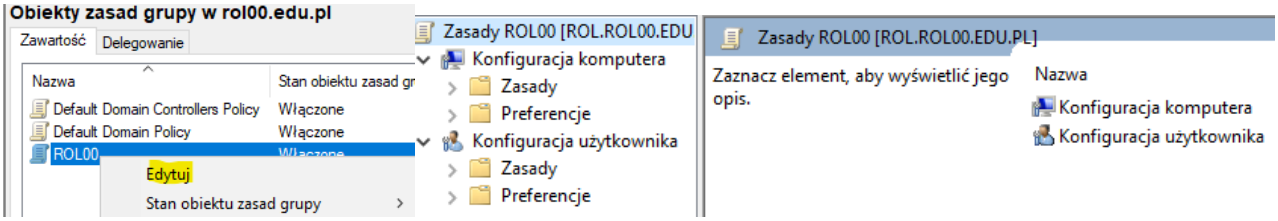
Kliknij prawym przyciskiem myszy kontener Group Policy Objecty (Obiekty zasad grupy) w drzewie konsoli i wybierz New (Nowe). Widok konsoli GPMC – tworzenie nowego obiektu zasad grupy (GPO)



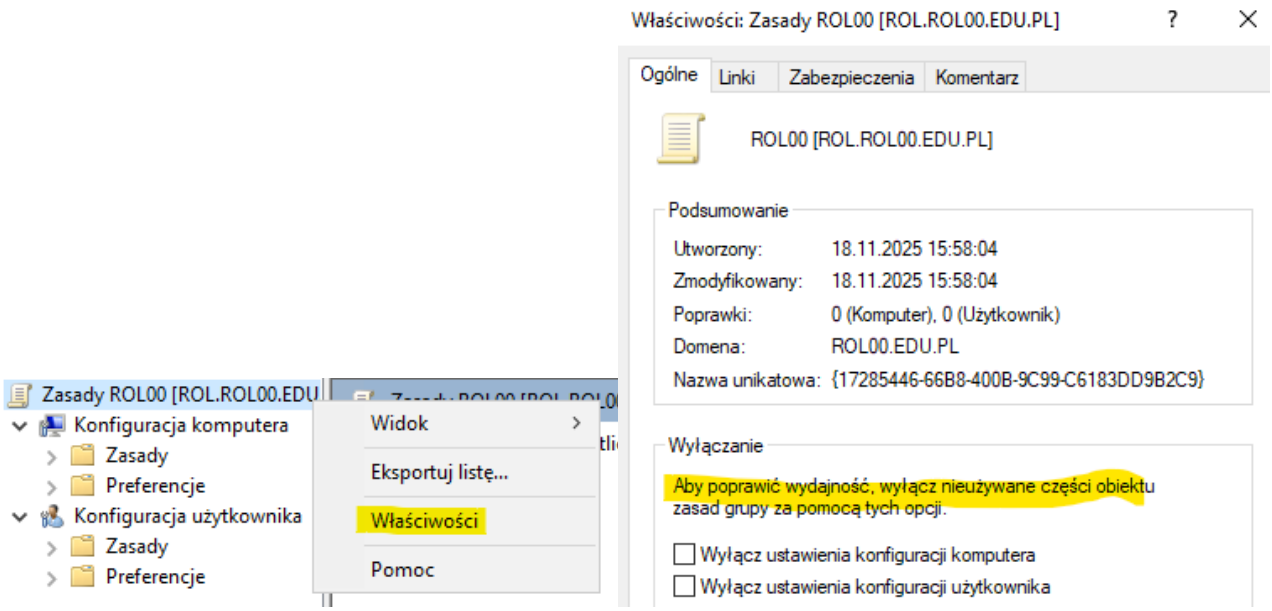
W polu Name (Nazwa) wpisz ROL00 gdzie 00 jest numerem twojego stanowiska



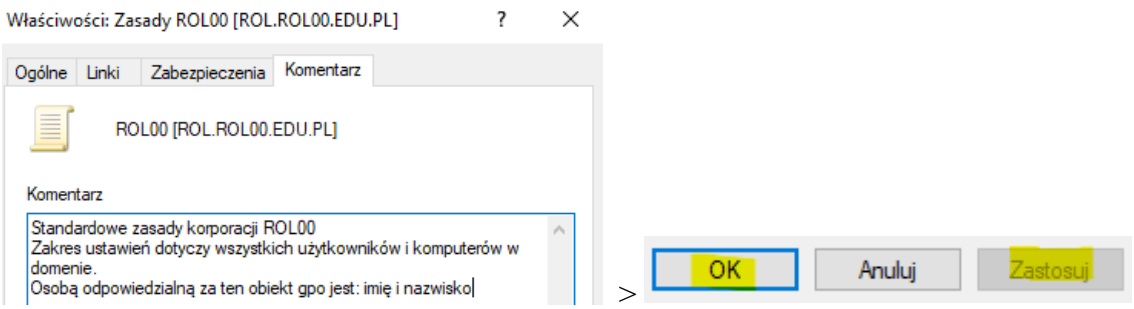
Kliknij prawym przyciskiem myszy ROL00 gdzie 00 jest numerem twojego stanowiska



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

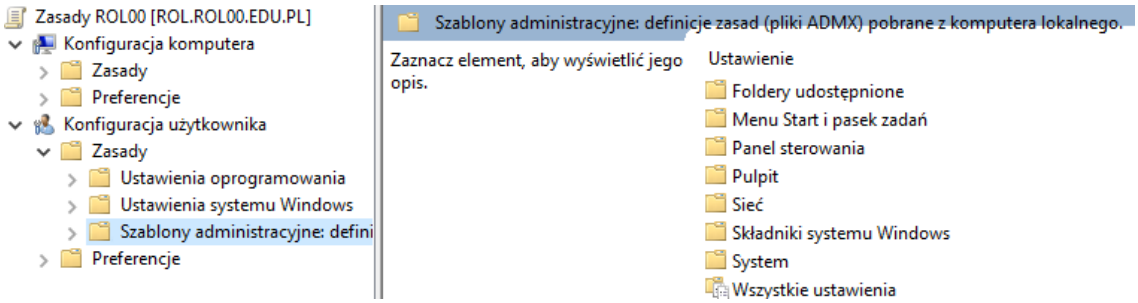


Kliknij zakładkę Comment (Komentarz) i wpisz jak poniżej



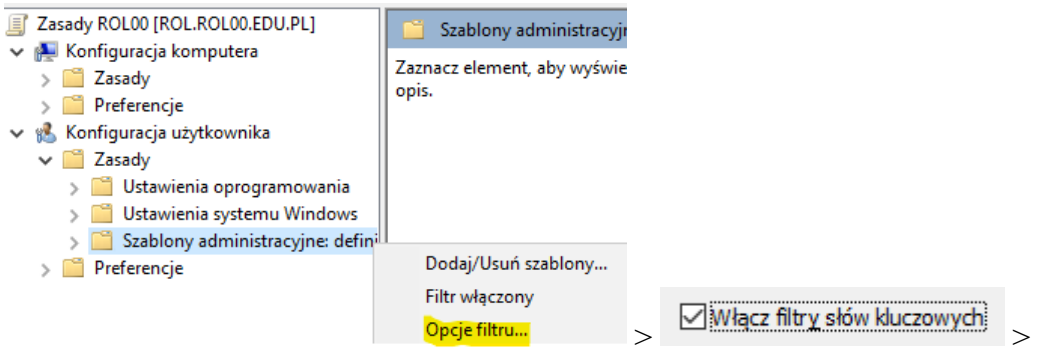
Skonfiguruj standardowe zasady korporacji, które określają, że komputery nie mogą być pozostawione bez opieki i w stanie zalogowania przez dłużej niż 10 minut, w tym celu:

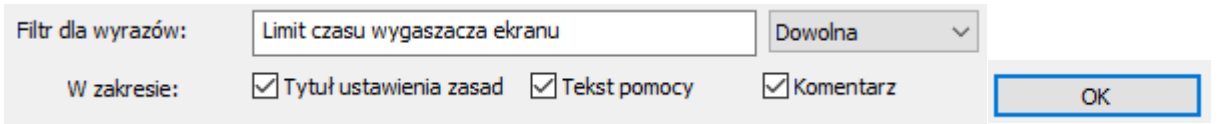
Rozwiń węzeł User Configuration\Policies\Administrative Templates (Konfiguracja użytkownika \Zasady\Szablony administracyjne). Widok węzła Szablony administracyjne w edytorze zasad grupy

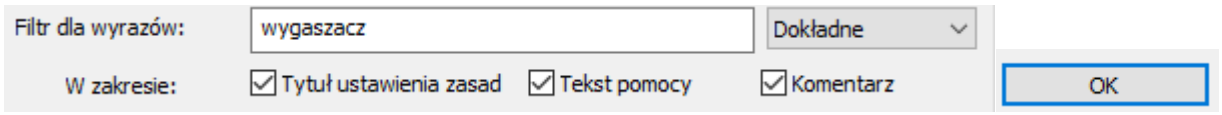


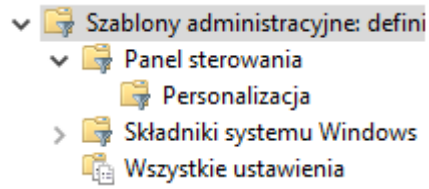
Przejrzyj ustawienia w tym węźle, zwróć szczególną uwagę na tekst wyjaśnień dla ustawień zasad, nie dokonuj żadnych zmian podczas tej czynności.

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



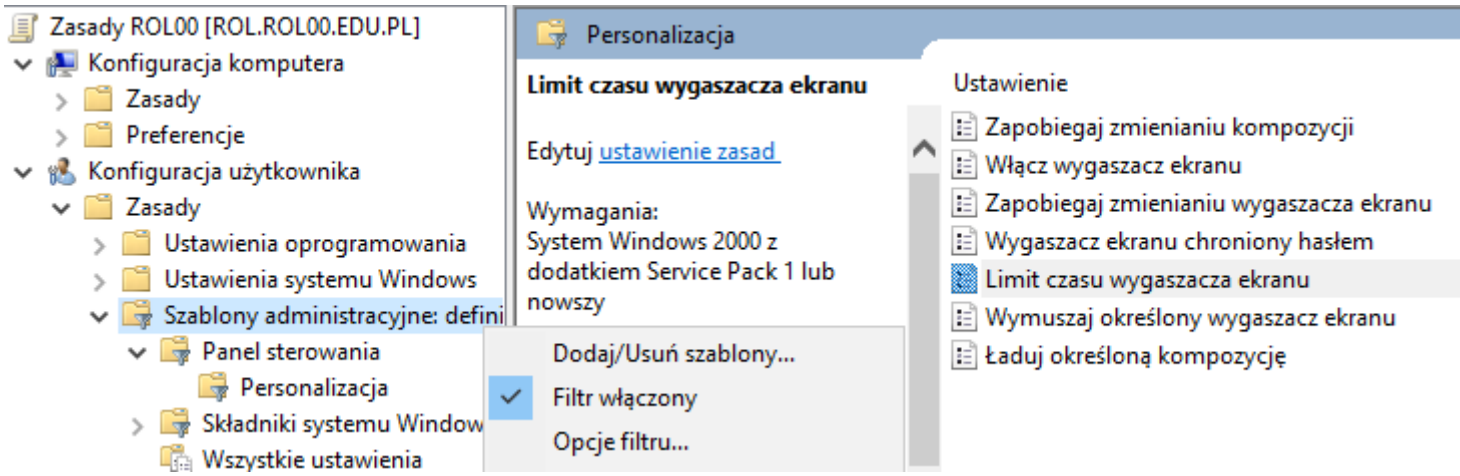




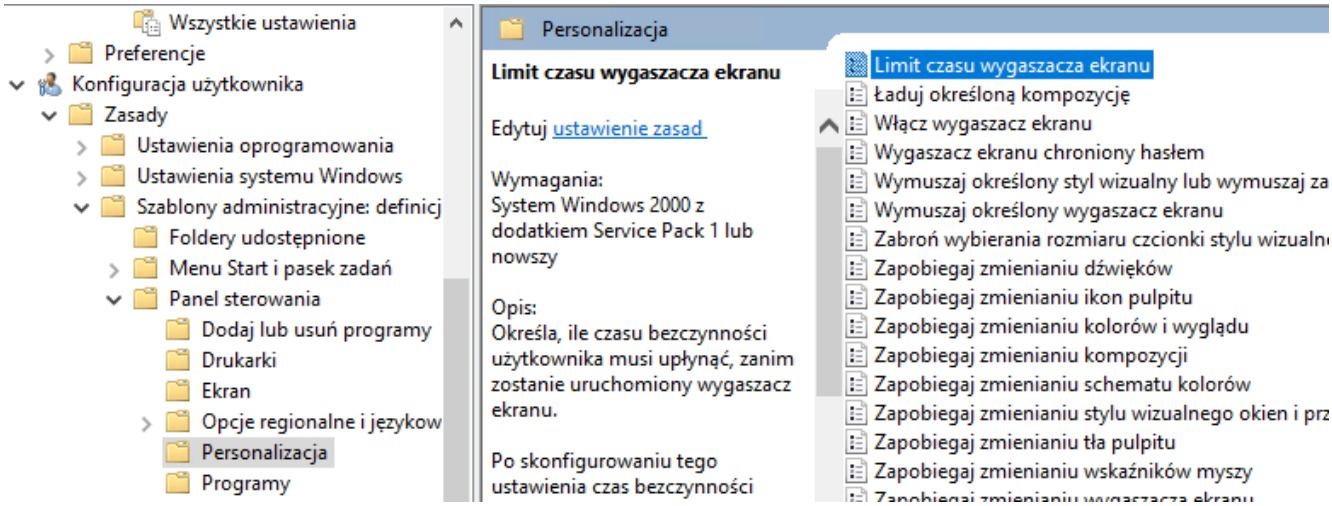


Lista ustawień po zastosowaniu filtru (screen saver)

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



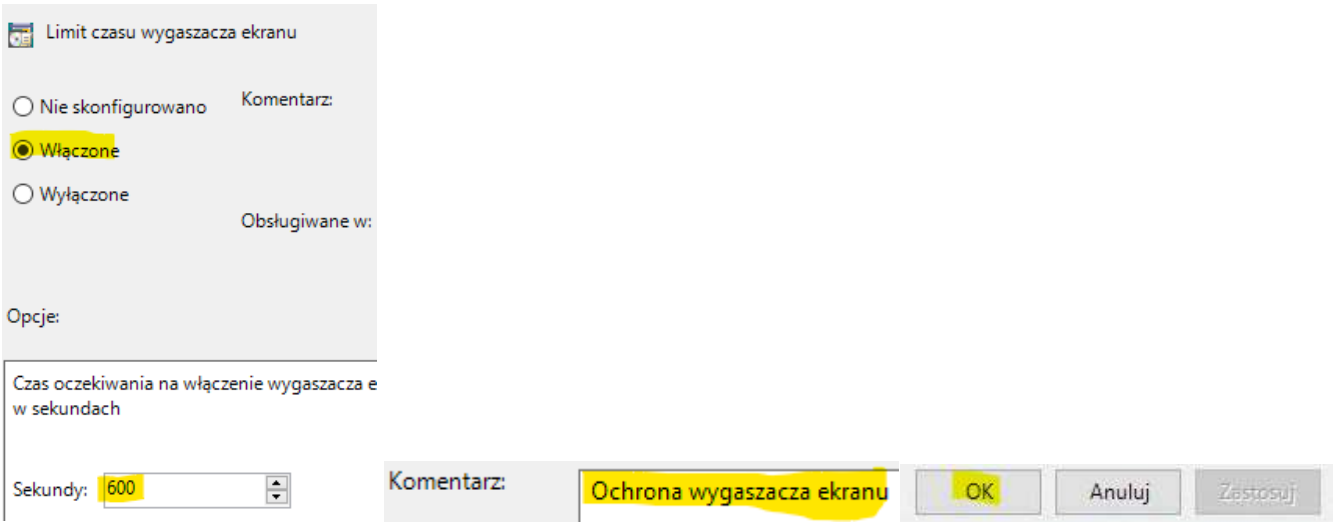
W węźle Control Panel\Display (Panel sterowania\Ekran) wybierz zasadę Screen Saver Timeout (Limit czasu wygaszacza ekranu).



Podwójnie kliknij zasadę Screen Saver timeout (Limit czasu wygaszacza ekranu), zwróć szczególną uwagę na tekst wyjaśnień:

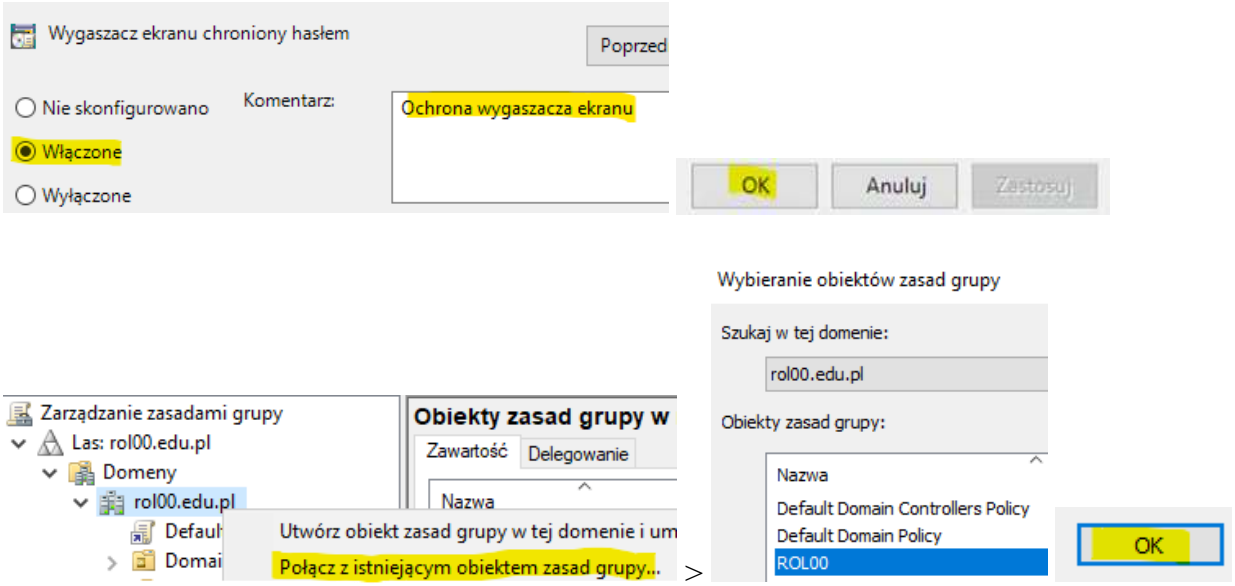
Określa, ile czasu bezczynności użytkownika musi upłynąć, zanim zostanie uruchomiony wygaszacz ekranu.
Po skonfigurowaniu tego ustawienia czas bezczynności można ustawić w zakresie od wartości minimalnej wynoszącej 1 sekundę do wartości maksymalnej wynoszącej 86 400 sekund (24 godziny). Jeżeli zostanie ustawiona wartość zero, wygaszacz ekranu nie będzie uruchamiany.
To ustawienie nie obowiązuje w następujących okolicznościach:
- *— Ustawienie jest wyłączone lub nie zostało skonfigurowane.*
- *— Czas oczekiwania jest ustawiony na zero.*
- *— Ustawienie Włącz wygaszacz ekranu jest wyłączone.*

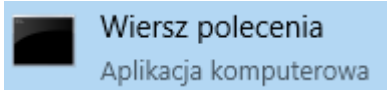
— *Ani w ustawieniu Nazwa pliku wykonywalnego wygaszacza ekranu, ani w oknie dialogowym Wygaszacz ekranu w aplecie Personalizacja lub Ekran w Panelu sterowania komputera klienckiego nie został określony prawidłowy program wygaszacza ekranu, który jest dostępny na komputerze klienckim. Jeżeli to ustawienie nie zostanie skonfigurowane, będzie używany dowolny czas oczekiwania ustawiony w oknie dialogowym Wygaszacz ekranu w aplecie Personalizacja lub Ekran w Panelu sterowania. Wartość domyślna to 15 minut.* Okno konfiguracji zasady „Screen Saver Timeout”



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

Okno konfiguracji zasady „Password protect the screen saver”



W 

wierszu polecenia wpisz

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

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

Wiersz polecenia – polecenie gpupdate /force /boot /logoff

Polecenie **gpupdate** służy do wymuszenia aktualizacji zasad grupy (Group Policy) w systemie Windows.

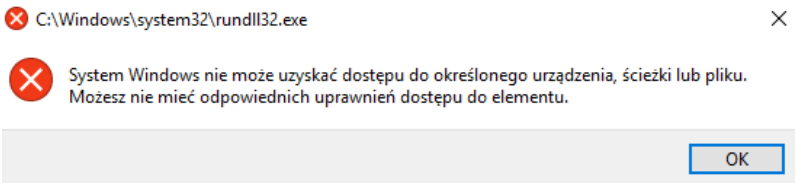
Parametry, które podałeś, mają konkretne znaczenie:

- **/force** – wymusza ponowne zastosowanie wszystkich zasad, nawet jeśli nie uległy zmianie. Bez tego parametru aktualizowane są tylko zmienione zasady.
- **/boot** – po zakończeniu aktualizacji wymusza restart komputera, jeśli jest to wymagane przez niektóre ustawienia (np. polityki dotyczące sterowników lub konfiguracji systemu).
- **/logoff** – po zakończeniu aktualizacji wymusza wylogowanie użytkownika, jeśli jest to wymagane przez niektóre ustawienia (np. polityki przypisane do profilu użytkownika).

⚠ **Ważne:** Parametry /boot i /logoff są opcjonalne i używa się ich w sytuacjach, gdy zmiany w zasadach wymagają ponownego uruchomienia lub wylogowania, aby zostały w pełni zastosowane.

Należy poczekać aż zostaną zaktualizowane zarówno zasady użytkownika, jak i zasady komputera.

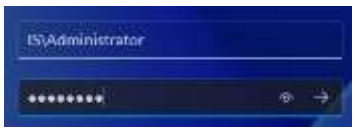
Na serwerze Wpisz w menu lupa > wygaszacz ekranu



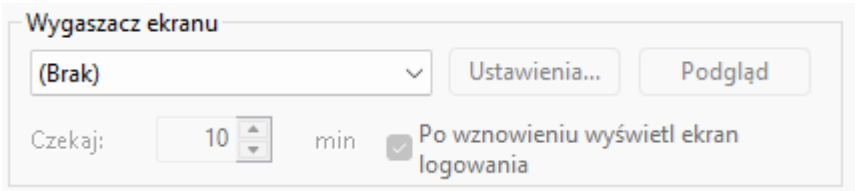
Widok ustawień wygaszacza ekranu na serwerze po zastosowaniu GPO

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

Uruchom klienta (stacje roboczą) Windows w wersji klienckiej (np. Windows 11), zaloguj się do konta Administrator domenowego na kliencie np. IS\Administrator.



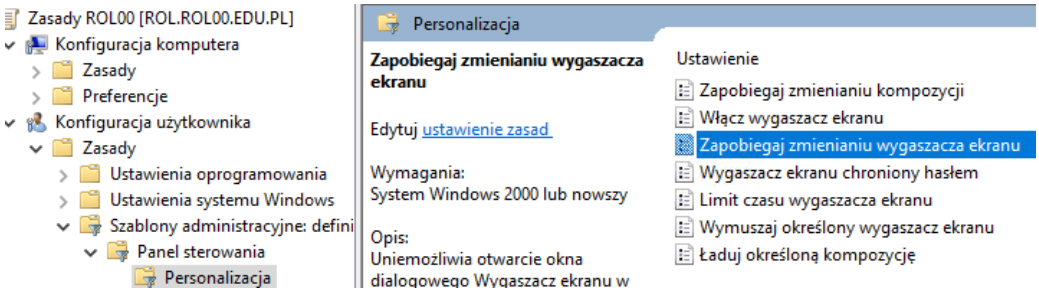
> Wpisz w menu lupa > wygaszacz ekranu >

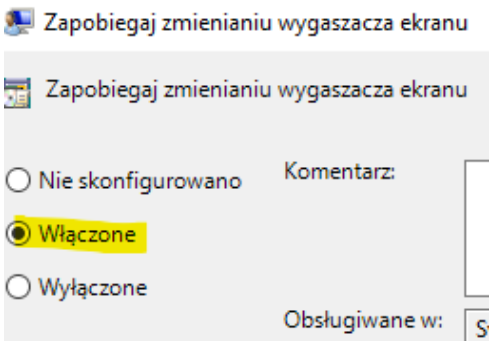


Widok ustawień wygaszacza ekranu na kliencie po zastosowaniu GPO

Wróć na serwer

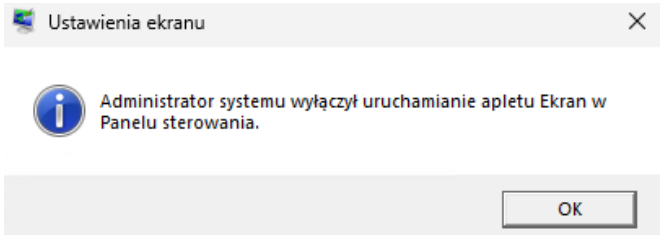
Ustaw Zapobiegaj zmienianiu wygaszacza ekranu





Wróć na stacje Windows 11

Wymuś aktualizacji zasad grupy gpupdate /force /boot /logoff



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 1b - Konfiguracja zasad GPO dla grupy Goście

Zakres działań:

1. Otwórz „**Użytkownicy i komputery usługi Active Directory**” (dsa.msc).
2. Kliknij prawym przyciskiem myszy na nazwę domeny i wybierz **Nowy > Jednostka organizacyjna**.
3. Wprowadź nazwę: **Goście** i zatwierdź.
4. Kliknij prawym przyciskiem myszy na nowo utworzoną jednostkę organizacyjną **Goście** i wybierz **Nowy > Użytkownik**.
5. Utwórz jednego lub więcej użytkowników tymczasowych (np. tymczasowy1, tymczasowy2).
6. Otwórz „**Zarządzanie zasadami grupy**” (gpmc.msc).

7. Kliknij prawym przyciskiem myszy na OU Goście i wybierz Utwórz nowy obiekt GPO w tej domenie i połącz go tutaj.
8. Nazwij obiekt zasad: **GPO_Goscie** i kliknij **OK**.
9. Kliknij prawym przyciskiem myszy na **GPO_Goscie** i wybierz **Edytuj**.
10. W edytorze zasad przejdź do:
    - **Konfiguracja użytkownika > Szablony administracyjne > Panel sterowania**
        - Włącz zasadę: Zabroń dostępu do Panelu sterowania i ustawień komputera.
    - **Konfiguracja użytkownika > Szablony administracyjne > Składniki systemu Windows > Eksplorator plików**
        - Włącz zasadę: **Zabroń dostępu do dysków z Mój komputer** i wybierz **Tylko dysk C**.
    - **Konfiguracja użytkownika > Szablony administracyjne > System > Opcje Ctrl+Alt+Del**
        - Włącz zasadę: **Usuń Menedżera zadań**.
11. Zamknij edytor zasad grupy.
12. Na stacji roboczej zalogowanej do domeny uruchom **Wiersz polecenia** i wpisz:

```
gpupdate /force
```

13. Zaloguj się jako użytkownik tymczasowy i sprawdź oraz udokumentuj, czy:
    - Panel sterowania jest zablokowany,
    - Dostęp do dysku C:\ jest zablokowany,
    - Menedżer zadań jest niedostępny.

Zapisz notatkę, w której powinny znaleźć się najważniejsze informacje dokumentujące cel i wykonane kroki, w skrócie.

Zadanie 1c - Blokowanie dostępu do Internetu przez GPO (wersja polska)

Wymagania wstępne

- Serwer z rolą Usługi domenowe Active Directory (Windows Server 2019).
- Zainstalowane narzędzie Zarządzanie zasadami grupy (GPMC).
- Włączona usługa Identyfikacja aplikacji (dla AppLocker).

Zakres działań:

Krok 1: Utworzenie grupy użytkowników

1. Otwórz Użytkownicy i komputery usługi Active Directory (dsa.msc).
2. Wybierz odpowiednią jednostkę organizacyjną (OU), np. „Uczniowie”.
3. Kliknij prawym przyciskiem myszy > Nowy > Grupa.
4. Nazwij grupę: Bez_Internetu.
5. Typ grupy: Zabezpieczeń, Zakres: Globalna.

6. Dodaj do grupy użytkowników, którym chcesz zablokować dostęp do Internetu.

Krok 2: Utworzenie obiektu GPO

1. Otwórz Zarządzanie zasadami grupy (gpmc.msc).
2. Wybierz jednostkę organizacyjną, z którą chcesz powiązać politykę.
3. Kliknij prawym przyciskiem myszy > Utwórz obiekt zasad grupy w tej domenie i połącz go tutaj.
4. Nazwij obiekt: Blokada_Internetu.

Krok 3: Edycja GPO

1. Kliknij prawym przyciskiem myszy na Blokada_Internetu > Edytuj.
2. Przejdź do:
    - Konfiguracja użytkownika > Zasady > Ustawienia zabezpieczeń > AppLocker > Reguły dla plików wykonywalnych\ *(jeśli AppLocker jest dostępny)*\ lub
    - Konfiguracja użytkownika > Ustawienia systemu Windows > Ustawienia zabezpieczeń > Zasady ograniczeń oprogramowania.

Krok 4: Utworzenie reguł odmowy

- W AppLocker:
    1. Kliknij Reguły dla plików wykonywalnych > Utwórz nową regułę.
    2. Typ reguły: Odmowa.
    3. Wskaż pliki dostępnej przeglądarki: chrome.exe, firefox.exe, msedge.exe, iexplore.exe.
    4. Zastosuj dla grupy Bez_Internetu.
- W Zasadach ograniczeń oprogramowania:
    1. Utwórz nowe reguły ścieżki dla plików przeglądarek.
    2. Ustaw poziom zabezpieczeń: Nie dozwolone.

Krok 5: Filtrowanie zabezpieczeń

1. W oknie GPO przejdź do zakładki Zakres.
2. W sekcji Filtrowanie zabezpieczeń usuń Użytkownicy uwierzytelnieni.
3. Dodaj grupę Bez_Internetu.

Krok 6: Test

1. Na stacji roboczej zaloguj się jako użytkownik z grupy Bez_Internetu.

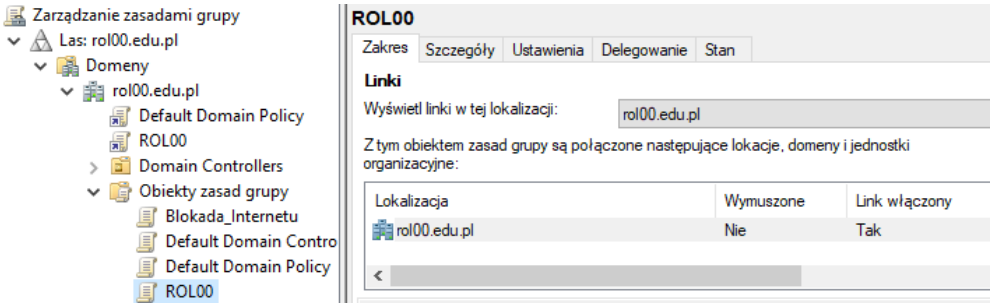
2. Wymuś aktualizację zasad: gpupdate /force
3. Spróbuj uruchomić przeglądarkę – powinna zostać zablokowana (komunikat o odmowie dostępu).

Efekt końcowy: Użytkownicy w grupie Bez_Internetu nie mogą uruchomić przeglądarek Chrome, Firefox, Edge.

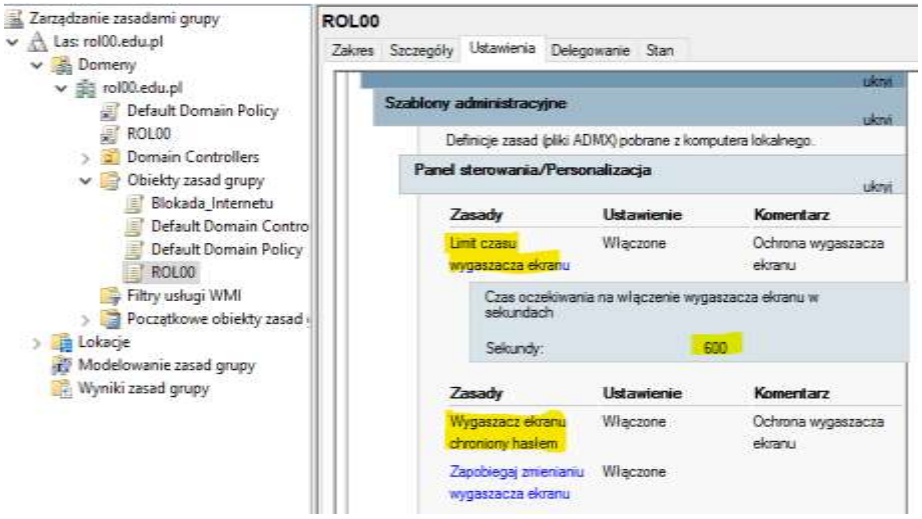
Zapisz notatkę, w której powinny znaleźć się najważniejsze informacje dokumentujące cel i wykonane kroki, w skrócie.

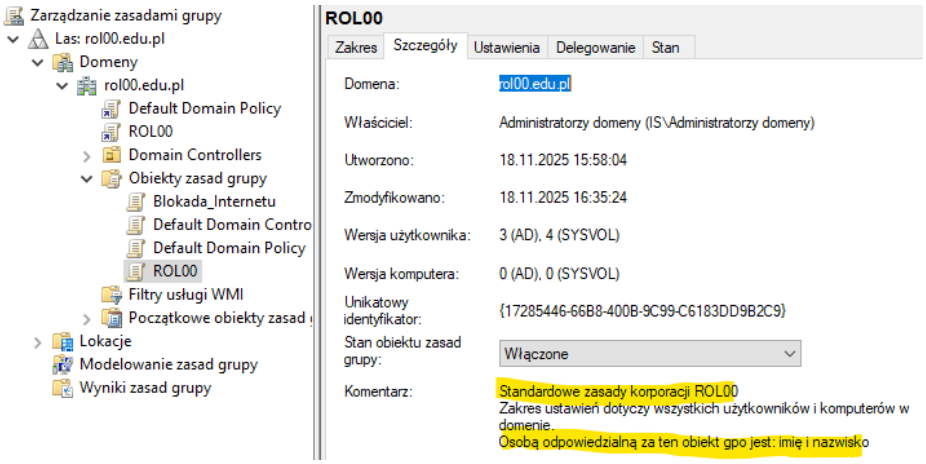
Zadanie 2

Badanie obiektu zasad grupy.



Kliknąć kartę **„Settings”** (Ustawienia), aby zobaczyć raport dotyczący ustawień zasad w tym obiekcie zasad grup. Jeśli na serwerze jest włączona funkcja Internet Explorer Enhanced Security Configuration (ESC), pojawi się komunikat z prośbą o dodanie strony about:security_mmc.exe do strefy Trusted Sites (Zaufane witryny), aby umożliwić wyświetlenie raportu. **show all**

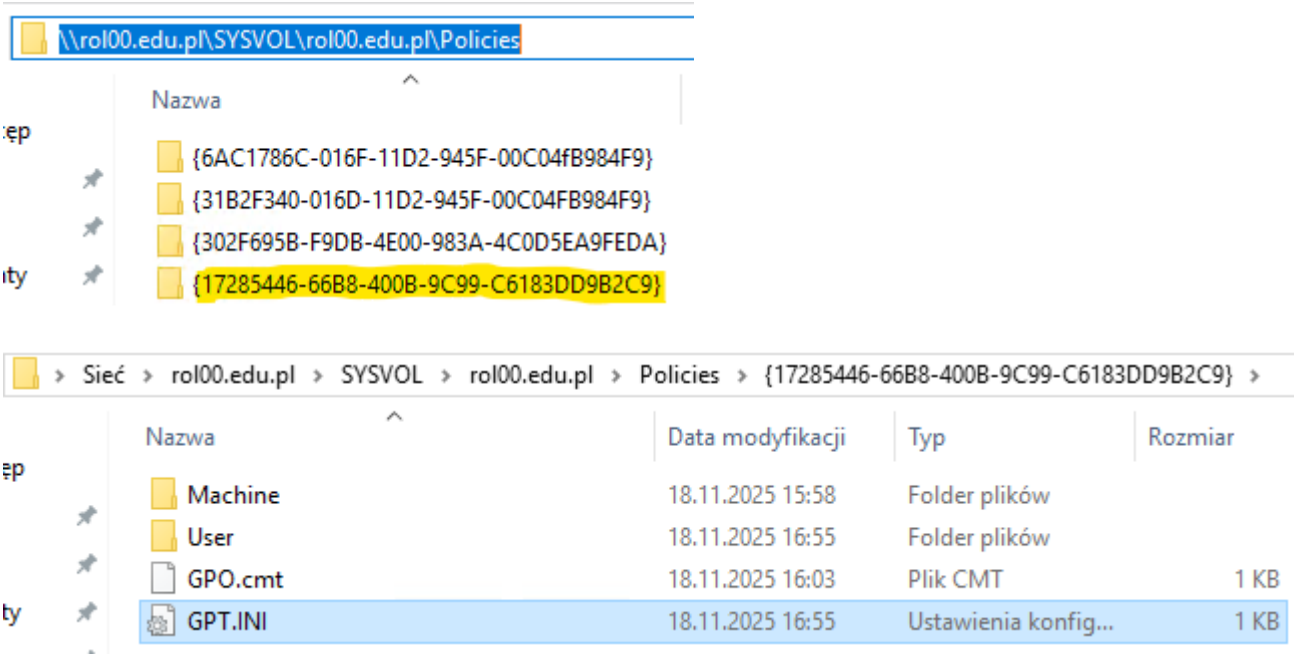




Zapisz unikatowy identyfikator obiektu pokazany na karcie Details (Szczegóły)

Np.: Unikatowy identyfikator: {17285446-66B8-400B-9C99-C6183DD9B2C9}

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



Jest to szablon GPT obiektu GPO. GPT (Group Policy Template) to część obiektu zasad grupy (GPO), która jest przechowywana w systemie plików w folderze SYSVOL na kontrolerze domeny. Szablon GPT zawiera fizyczne pliki i dane konfiguracyjne powiązane z GPO.

Składniki GPT:

Pliki .pol - zawierają ustawienia zasad (np. dla użytkownika i komputera).

Folder Machine - ustawienia zasad dla komputera.

Folder User - ustawienia zasad dla użytkownika.

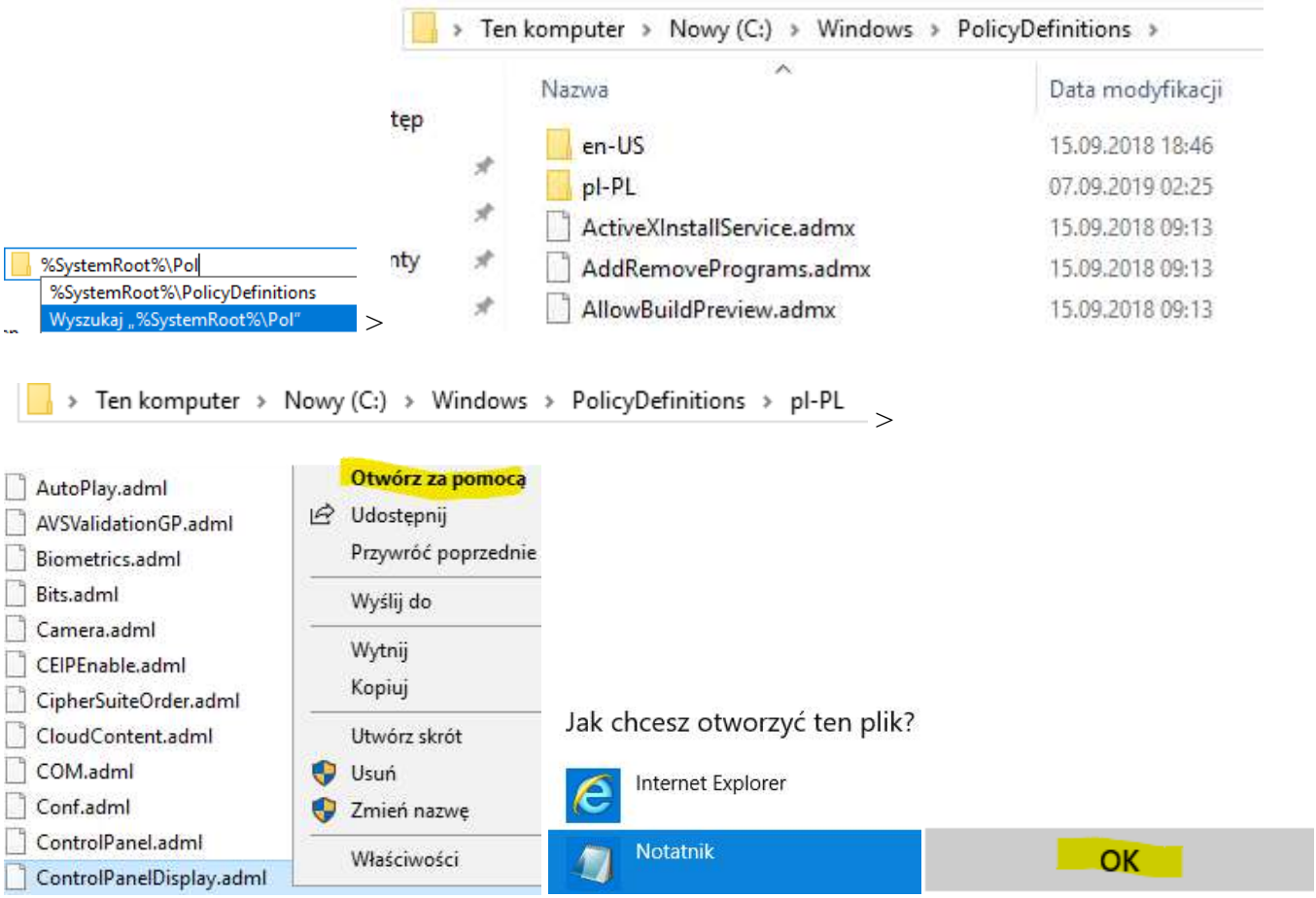
Plik GPT.ini - zawiera wersję GPO i inne metadane.

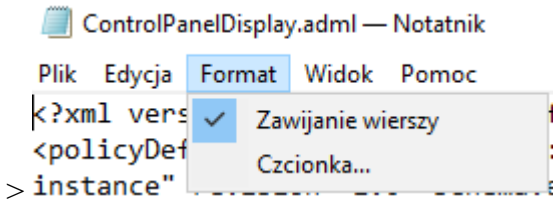
Lokalizacja: \\<nazwa_domeny>\SYSVOL\<nazwa_domeny>\Policies\<GUID_GPO>
gdzie GUID_GPO to unikalny identyfikator obiektu zasad grupy.
Rola: Szablon GPT jest używany przez system Windows do replikacji zasad między kontrolerami domeny oraz do stosowania zasad na komputerach klienckich.
Zapisz notatkę.

Zadanie 3

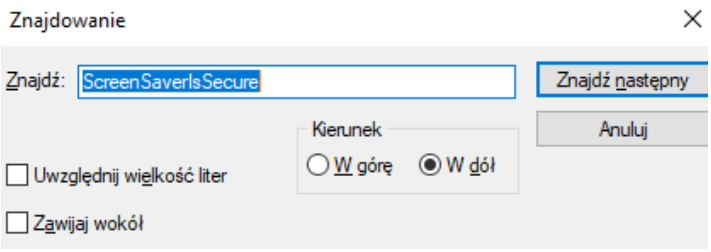
Badanie szablonów administracyjnych.

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.





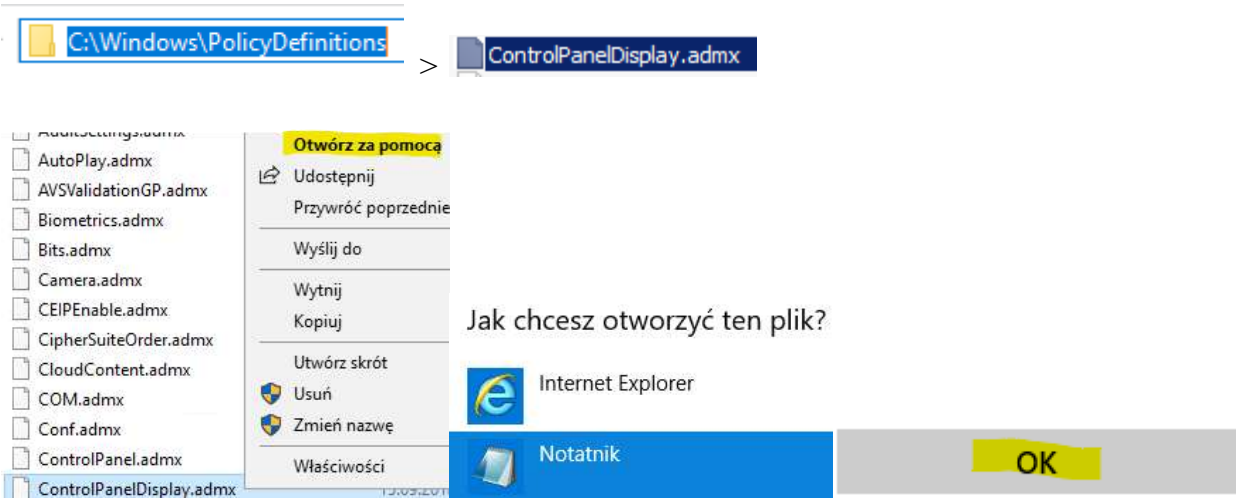
Wyszukaj tekst: ScreenSaverIsSecure



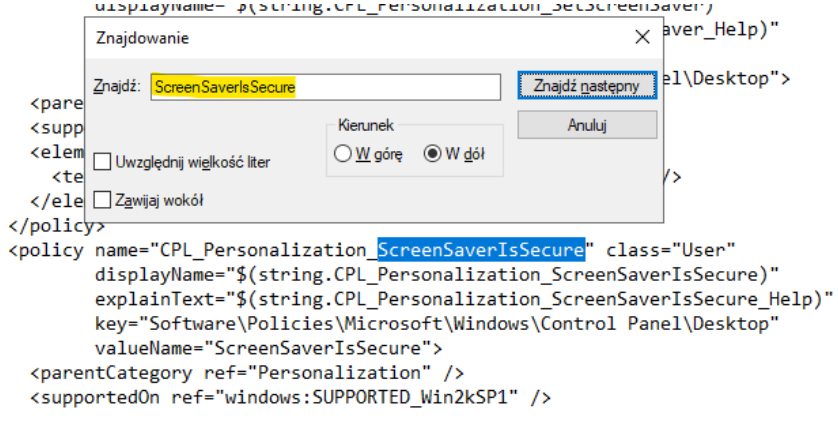
SaverIs > I to jest duża litera I jak Irek

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

Zamknij plik i przejdź do folderu jak poniżej



Wyszukaj tekst




```
</policy>
<policy name="CPL_Personalization_ScreenSaverIsSecure" class="User"
        displayName="$(string.CPL_Personalization_ScreenSaverIsSecure)"
        explainText="$(string.CPL_Personalization_ScreenSaverIsSecure_Help)"
        key="Software\Policies\Microsoft\Windows\Control Panel\Desktop"
        valueName="ScreenSaverIsSecure">
  <parentCategory ref="Personalization" />
  <supportedOn ref="windows:SUPPORTED_Win2kSP1" />
```

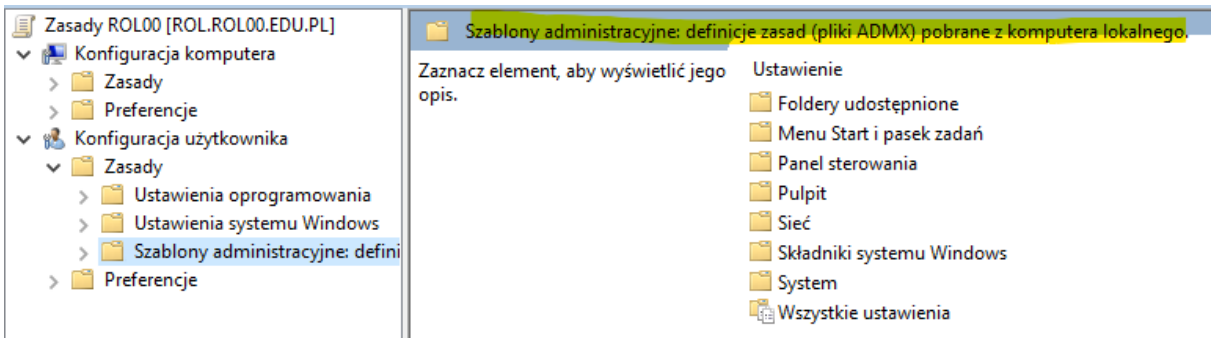
Zidentyfikuj następujące elementy, zapisz je do zeszytu:

- 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

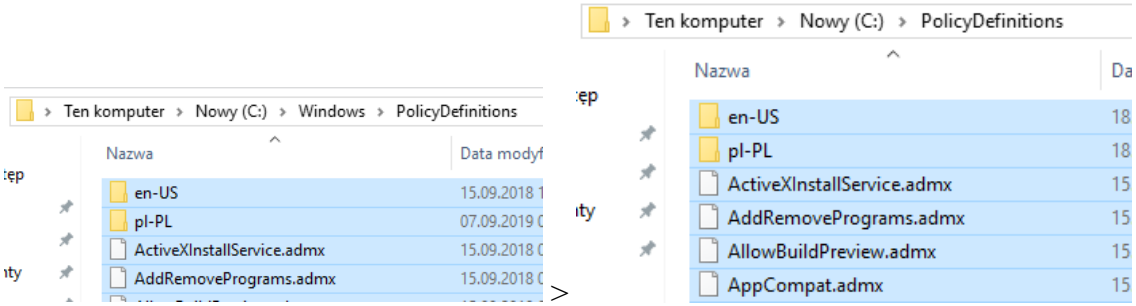
Tworzenie magazynu centralnego.

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.



Zapisz notatkę, w której powinny znaleźć się kluczowe informacje, które dokumentują wykonane kroki oraz cel zadania. Wykonane kroki (skrótowo, kilka słów):
Sprawdzenie źródła szablonów. Węzeł „Szablony administracyjne” w GPO pobierał pliki z komputera lokalnego.
Zamknięcie konsoli GPMC (Zarządzanie zasadami grupy).
Utworzenie folderu magazynu centralnego
Ścieżka: \\<domena>\SYSVOL\<domena>\Policies\PolicyDefinitions
Skopiowanie plików szablonów z lokalnego folderu: %SystemRoot%\PolicyDefinitions do folderu w SYSVOL.
Uwzględnienie plików językowych Folder pl-PL (dla polskiej wersji).
Weryfikacja. Po ponownym otwarciu edytora GPO, szablony pobierane są z magazynu centralnego.

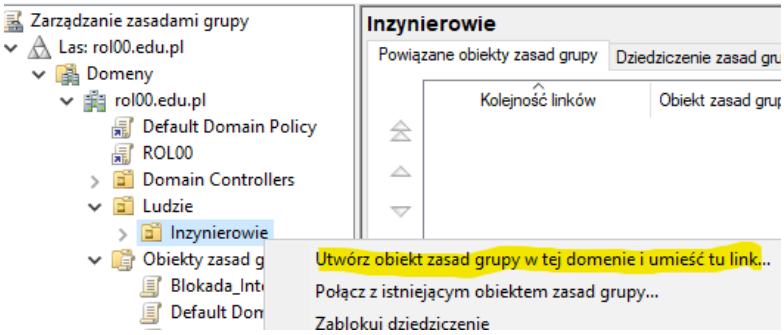
Zadanie 5

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

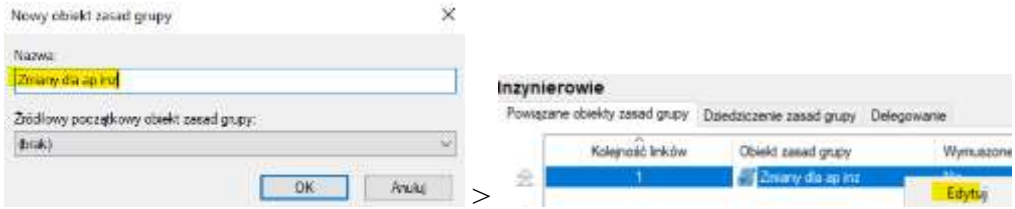
Obiekt zasad grupy ROL00, przyłączony do domeny, konfiguruje ustawienia zasad wymagające 10-minutowego okresu przed włączeniem się wygaszacza ekranu. Pewien inżynier zgłasza, że krytyczna aplikacja wykonująca długotrwałe obliczenia zawiesza się, gdy uruchomi się wygaszacz ekranu i prosi o niestosowanie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

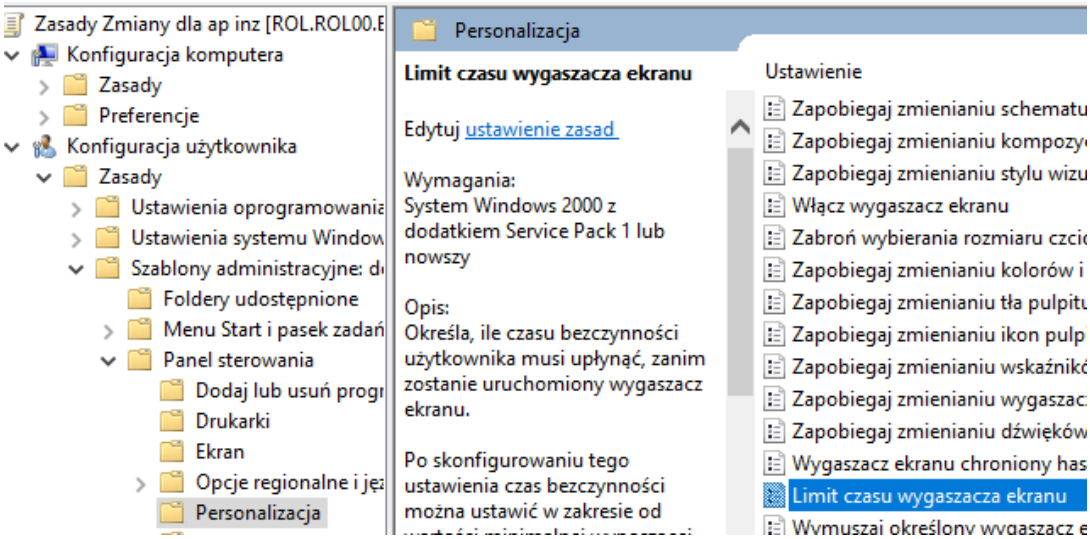
Konflikt zasad wygaszacza ekranu dla zespołu inżynierów i jego rozwiązanie.

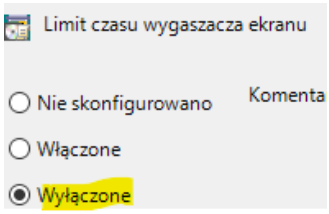
Widok konfiguracji zasad dla zespołu inżynierów.

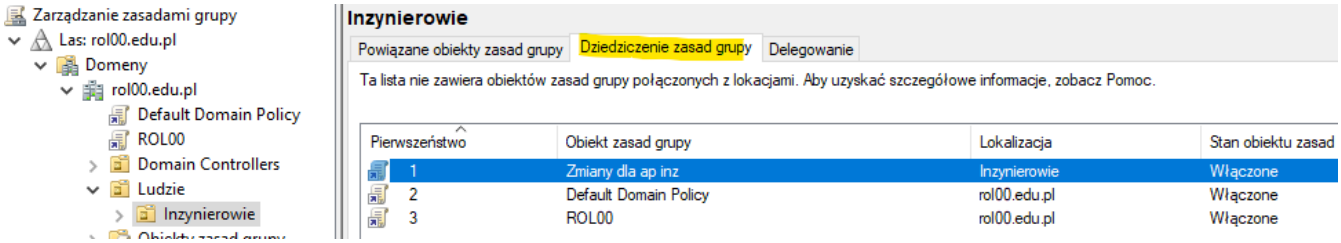


Utwórz obiekt zasad grupy „Zmiany dla ap inz”









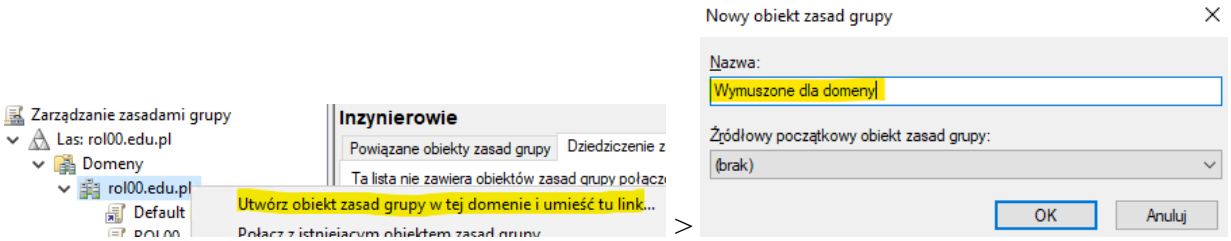
Zwrócić uwagę, że obiekt zasad grupy Zmiany dla ap inz ma pierwszeństwo przed obiektem zasad grupy ROL00.
Skonfigurowane przez nas ustawienie, które jawnie wyłącza wygaszacz ekranu, uchyli ustawienie w obiekcie zasad grupy ROL00.
Obiekt Zmiany dla ap inz ma pierwszeństwo przed obiektem zasad grupy ROL00.

Zapisz notatkę. Co wpisać w notatce (kilka słów – esencja):
Cel: Wymuszenie zasady „Zawsze czekaj na sieć" dla wszystkich systemów.
Lokalizacja ustawienia: Konfiguracja komputera → Szablony administracyjne → System → Logowanie.
Działanie: Włączono ustawienie „Zawsze czekaj na sieć podczas uruchamiania komputera i logowania".
Zastosowano opcję Enforced (Wymuszone) na obiekcie GPO Wymuszone zasady domenowe.
Efekt: Polityka ma pierwszeństwo przed innymi GPO, nie można jej uchylić.
Zapewnia synchronizację zasad przy logowaniu.

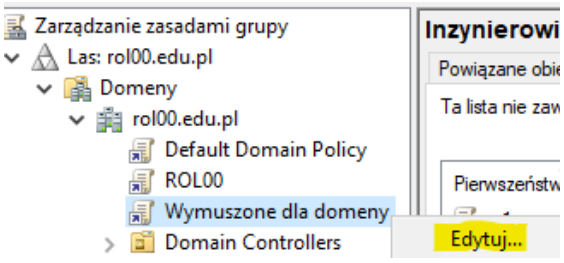
Zadanie 6

Konfigurowanie opcji Enforced (Wymuszenie)

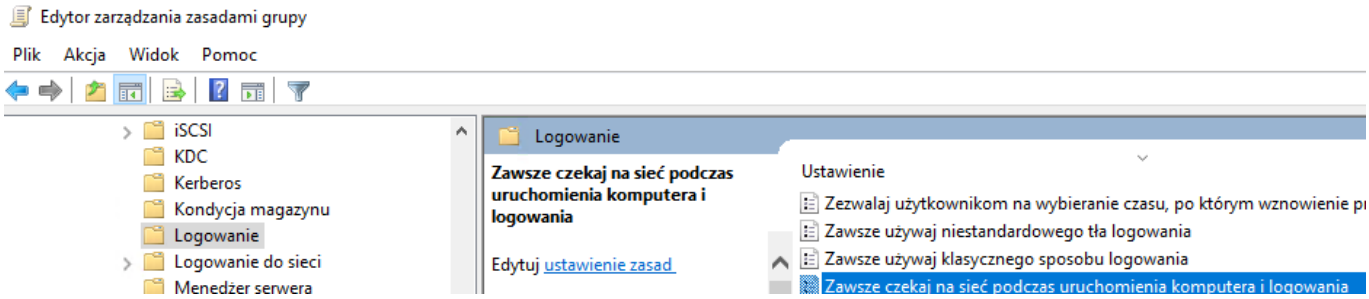
Zapewnij, aby wszystkie systemy uzyskiwały zmiany zasad grupy tak szybko jak to możliwe.
W tym celu należy włączyć ustawienie zasad grupy Always Wait for The Network (Zawsze czekaj na sieć). Administratorzy nie mogą uchylać tego ustawienia, musi być ono wymuszane dla wszystkich systemów.



>



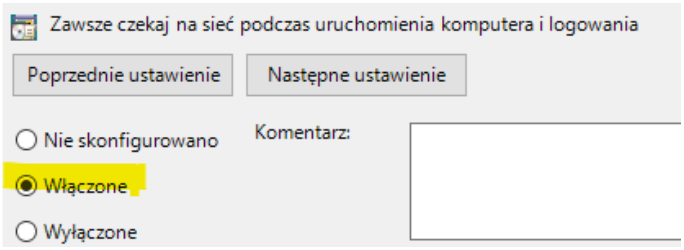
> Lokalizacja w GPO: Konfiguracja komputera > Szablony administracyjne > System > Logowanie



Widok zasady „Zawsze czekaj na sieć podczas uruchamiania komputera i logowania”

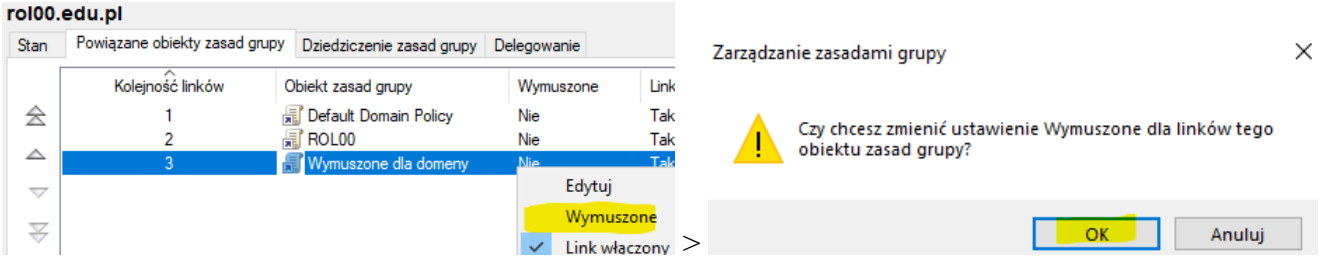
Podwójnie kliknij ustawienie zasad Always Wait for The Network At Computer Startup And Logon (Zawsze czekaj na sieć podczas uruchomienia komputera i logowania).

Włączenie zasady *Always Wait for The Network* (Zawsze czekaj na sieć podczas uruchamiania komputera i logowania) dla szybkiego stosowania zasad.



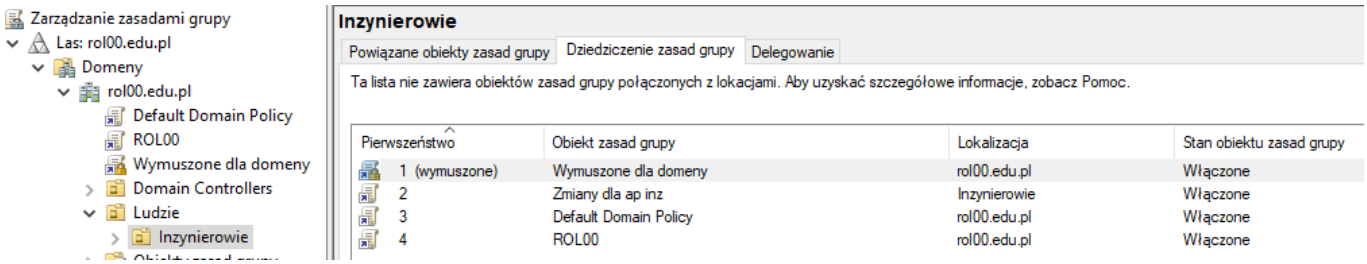
Zamknąć Edytor zarządzania zasadami grupy.

Kliknąć prawym przyciskiem myszy obiekt zasad grupy Wymuszone zasady domenowe i wybrać Enforced (Wymuszone). Wymuszenie zasad domenowych poprzez opcję *Enforced*.



Kolejność linków	Obiekt zasad grupy	Wymuszone	Link włączony	Stan obiektu zasad grupy
1	Default Domain Policy	Nie	Tak	Włączone
2	ROL00	Nie	Tak	Włączone
3	Wymuszone dla domeny	Tak	Tak	Włączone

Zaznaczyć jednostkę organizacyjną Inżynierowie, a następnie kliknąć kartę Group Policy Inheriiance (Dziedziczenie zasad grupy). Wymuszenie zasad domenowych poprzez opcję Enforced.



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

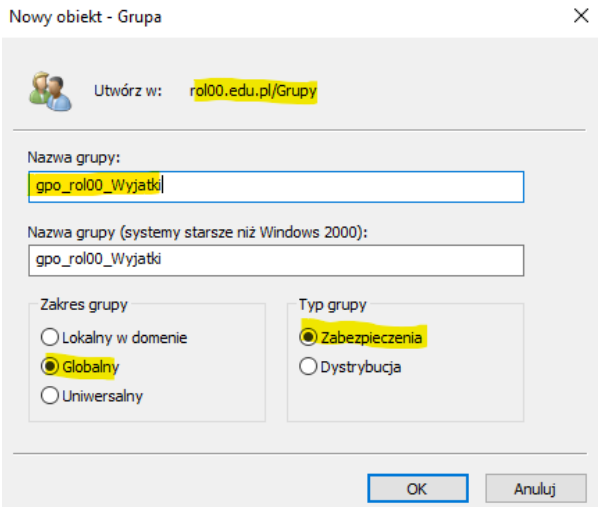
Zapisz notatkę. W notatce powinny znaleźć się najważniejsze informacje dokumentujące cel i wykonane kroki, w skrócie, tak jak w poprzednich zadaniach: Cel zadania: Zapewnienie, aby wszystkie systemy w domenie stosowały zmiany zasad grupy natychmiast i aby ustawienie „Zawsze czekaj na sieć" było wymuszone, bez możliwości uchylenia przez inne GPO.
Kluczowe informacje (kilka słów)

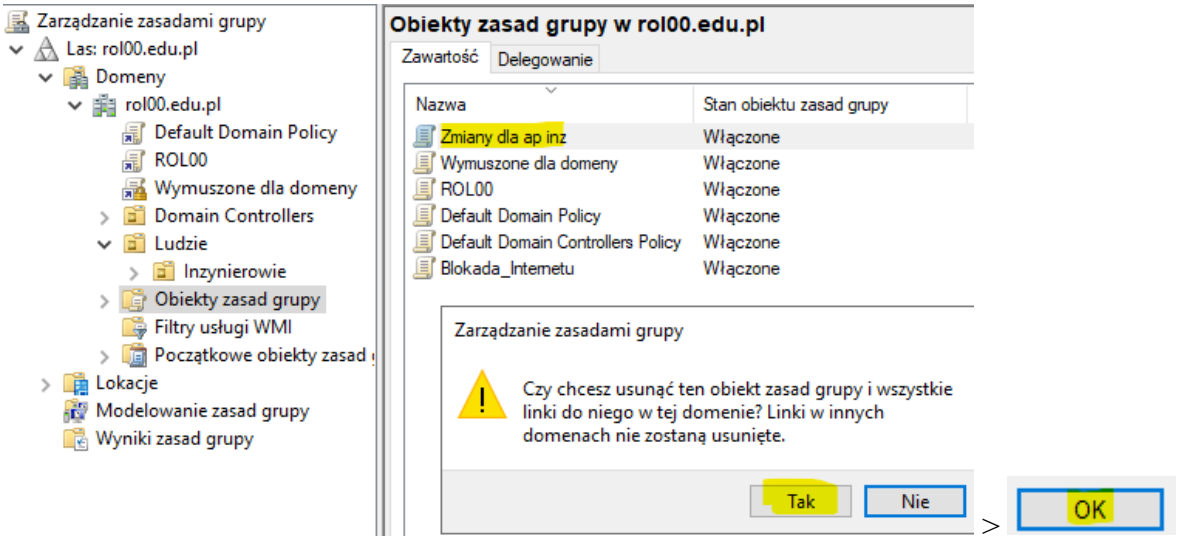
- Lokalizacja ustawienia: *Konfiguracja komputera → Szablony administracyjne → System → Logowanie.*
- Działanie:
  - Włączono zasadę „Zawsze czekaj na sieć podczas uruchamiania komputera i logowania".
  - Zamknięto Edytor GPO.
  - Na obiekcie Wymuszone zasady domenowe zastosowano opcję Enforced (Wymuszone).
- Sprawdzenie dziedziczenia:
  - W jednostce organizacyjnej „Inżynierowie" potwierdzono, że wymuszony GPO ma pierwszeństwo przed innymi.
- Efekt:
  - Ustawienie jest stosowane na wszystkich komputerach w domenie, nie można go nadpisać innymi GPO.

Zadanie 7

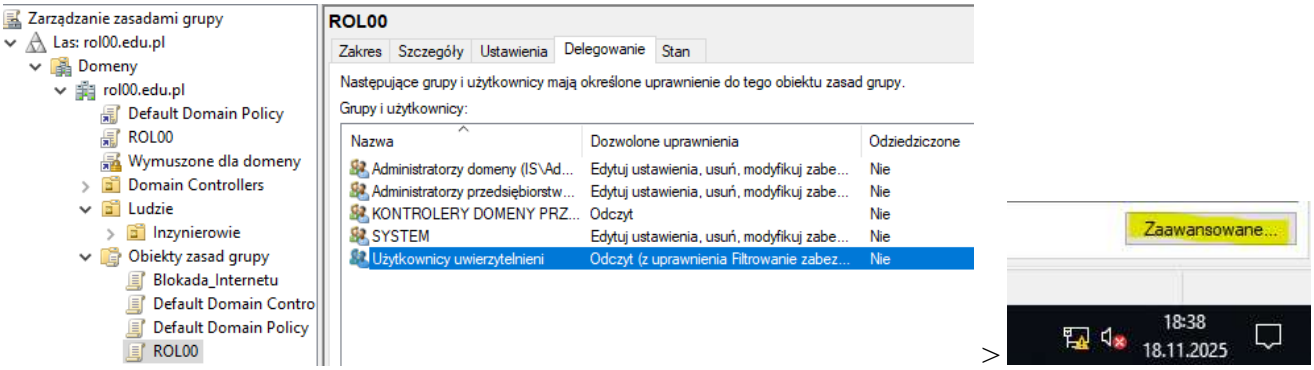
Konfigurowanie filtrowania zabezpieczeń.

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

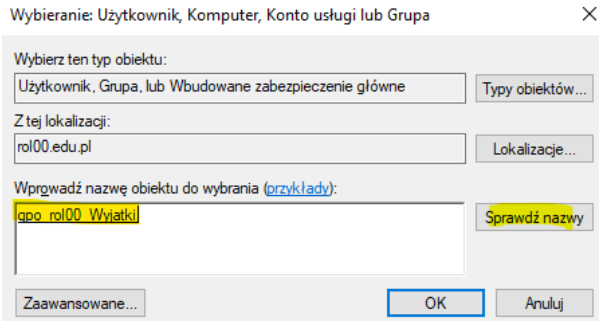


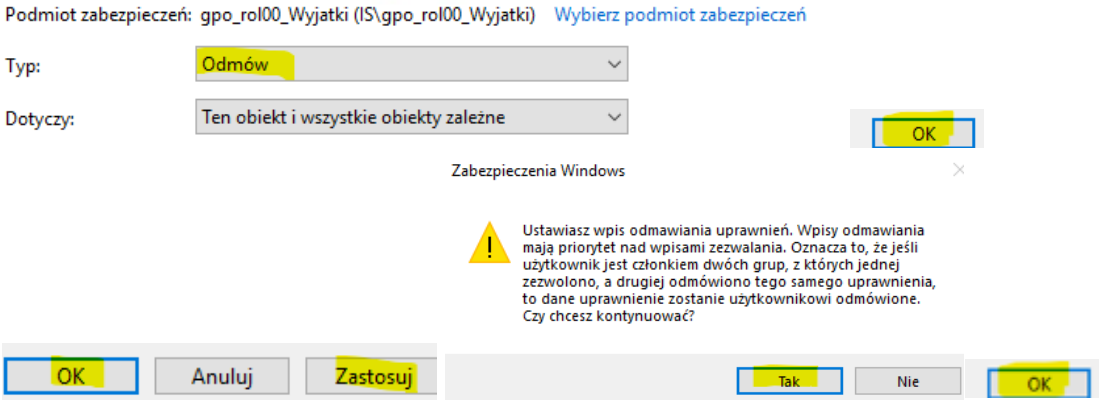


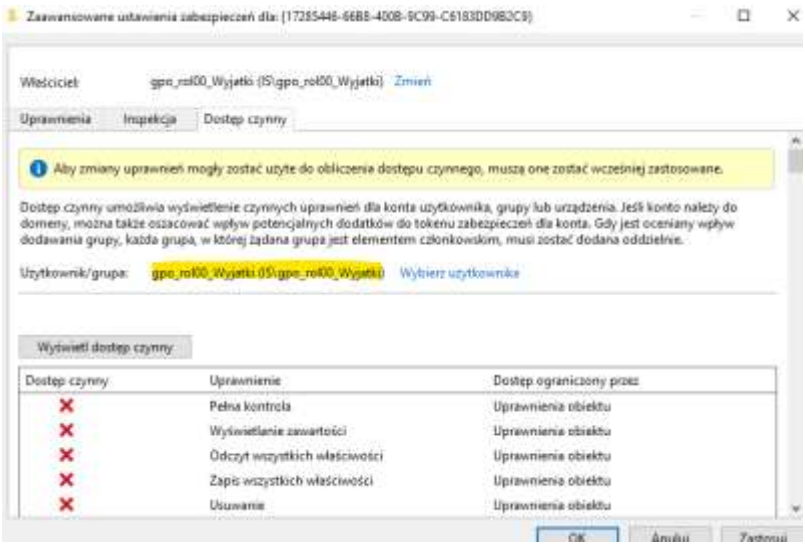
Zaznacz obiekt zasad grupy ROL00 w kontenerze Group Policy Objects (Obiekty zasad grupy)

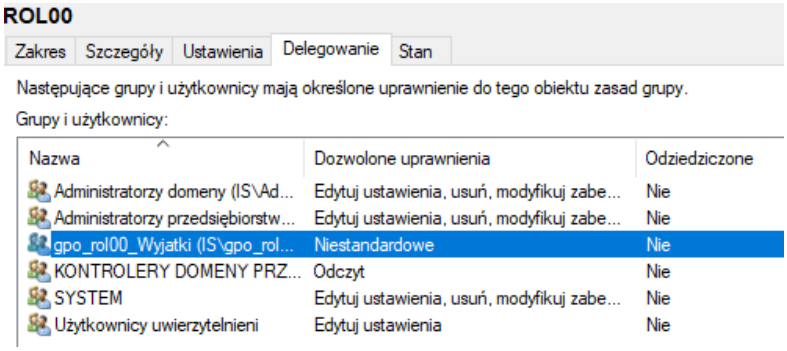


> Dodaj > Podmiot zabezpieczeń: Wybierz podmiot zabezpieczeń

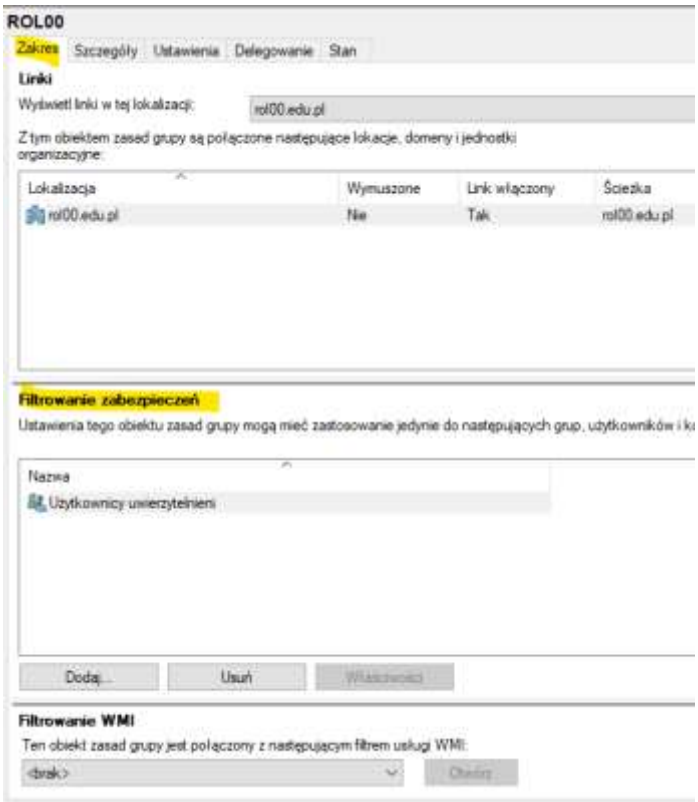








Kliknij kartę Scope (Zakres) i zbadaj sekcję Security Filtering (Filtrowanie zabezpieczeń).



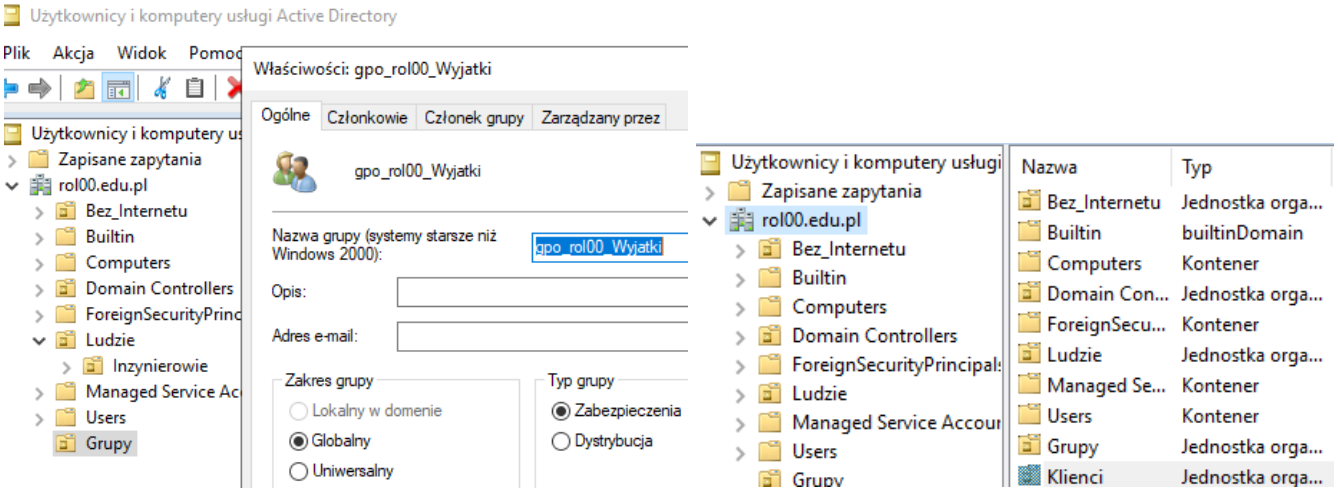
Domyślne filtrowanie zabezpieczeń dla nowego obiektu zasad grupy jest takie, że grupa Authenticated Users (Użytkownicy uwierzytelnieni) ma uprawnienie Allow Apply Group Policy (Zezwalaj Stosowanie zasad grup), więc wszyscy użytkownicy i komputery w zakresie tego łącza do obiektu GPO będą stosować ustawienia 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.

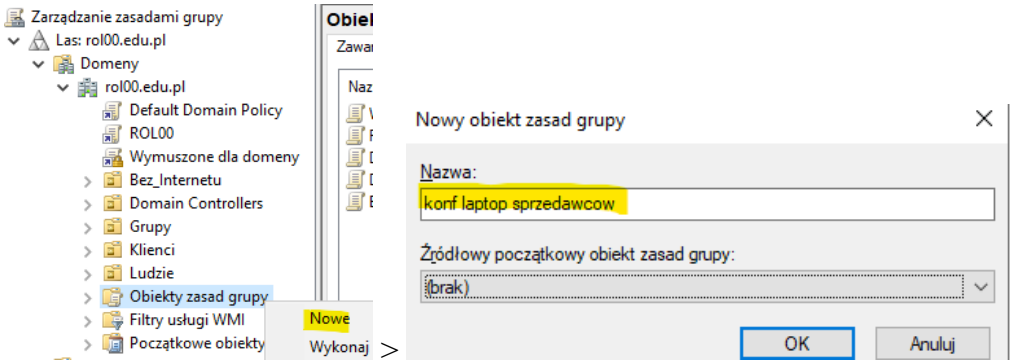
Zapisz notatkę. Zapisz w zeszycie na czym polega filtrowanie zabezpieczeń.

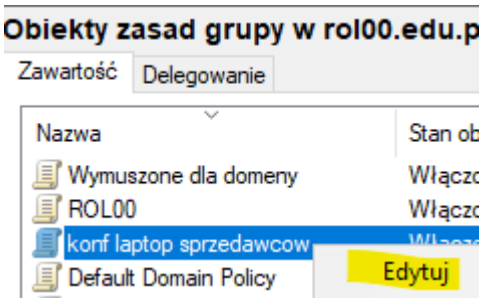
Zadanie 8

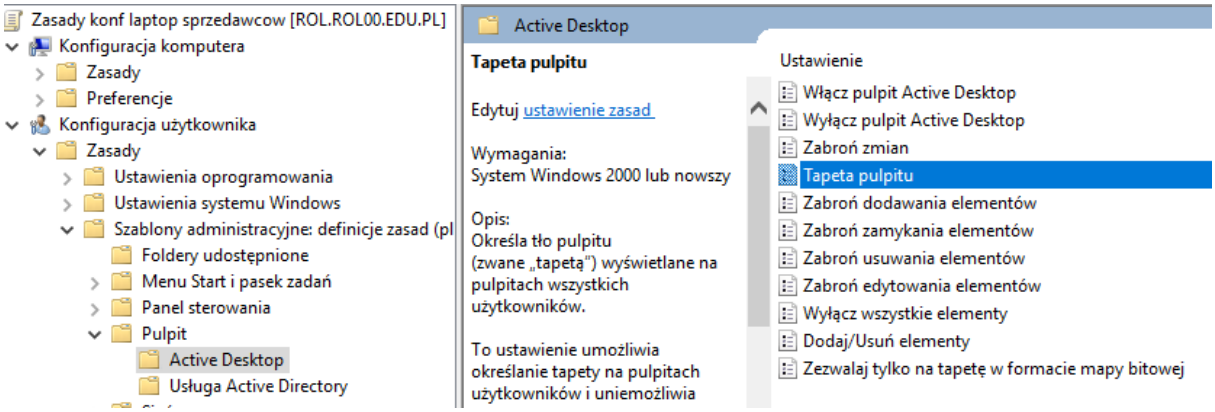
Przetwarzanie zasad w sprzężeniu zwrotnym.

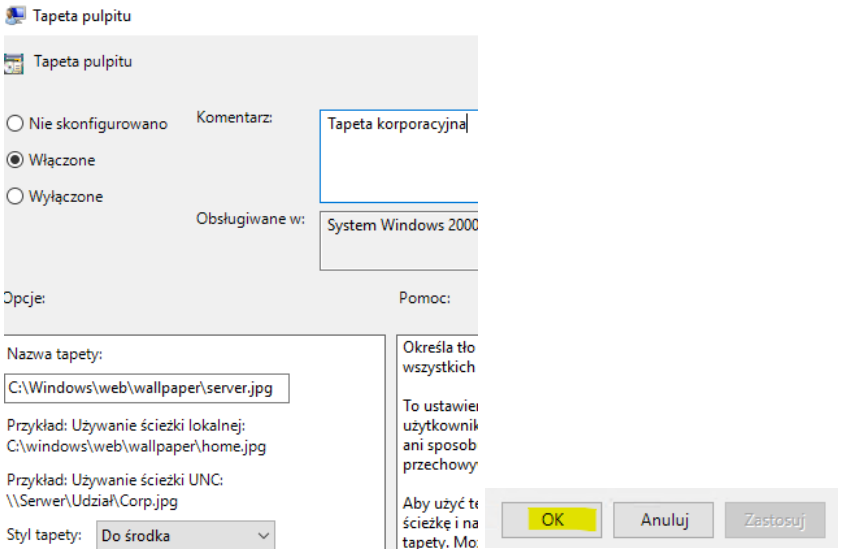
Sprzedawca w firmie ROL00 włączył swój komputer, aby przeprowadzić prezentację dla ważnego klienta, a na tapecie pulpitu był obraz, który świadczył o wątpliwym guście tego sprzedawcy.
Zarząd poprosił o zapewnienie, żeby laptopy używane przez sprzedawców, gdy są oni zalogowani nie miały tapety, nie jest 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.



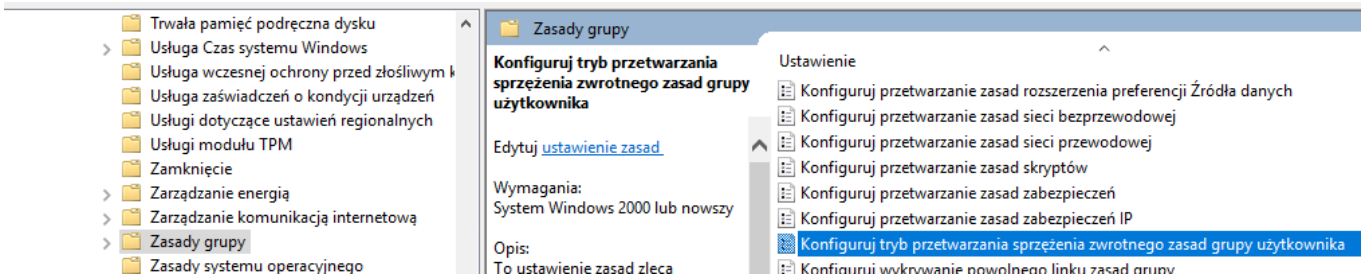




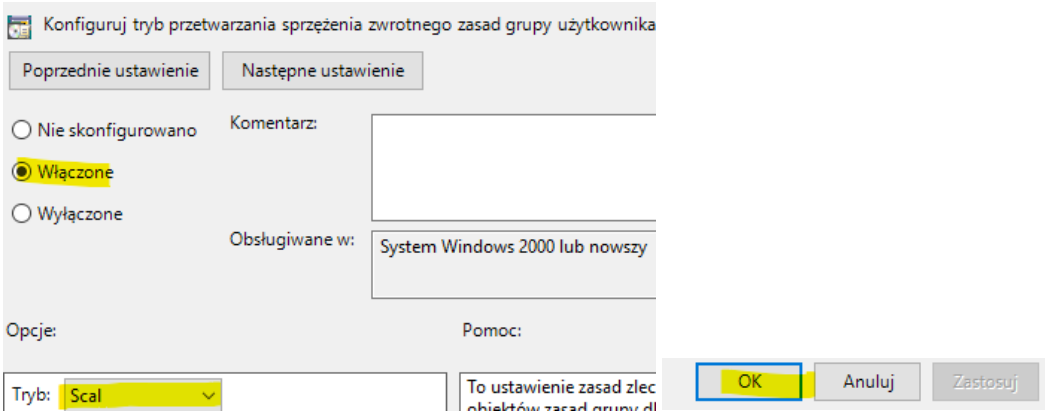




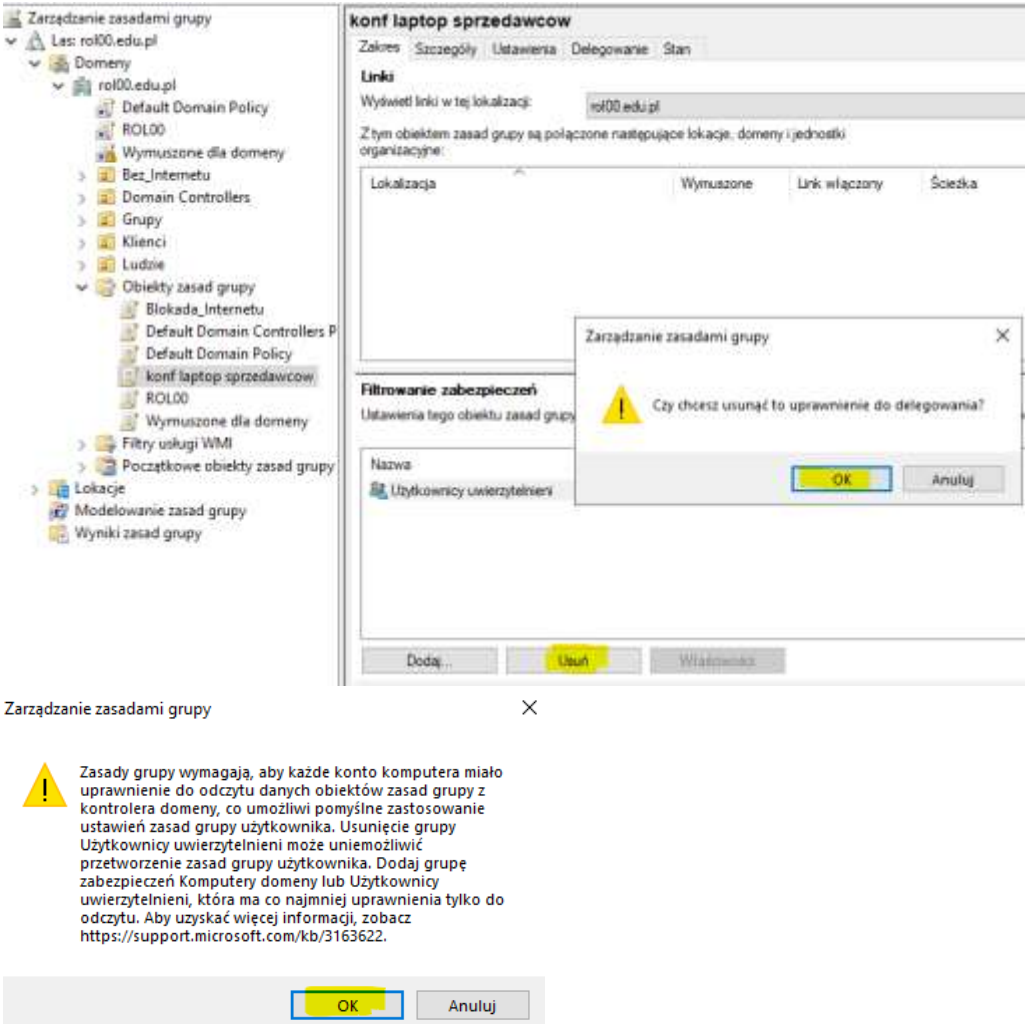
Rozwinąć węzeł Computer Configuration\Policies\Administrative Templates\System\Group Policy (Konfiguracja komputera\Zasady\Szablony administracyjne\System\Zasady grupy).
Podwójnie kliknąć ustawienie zasad User Group Policy Loopback Proeessing Mode (Konfiguruj tryb przetwarzania sprzężenia zwrotnego zasad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



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

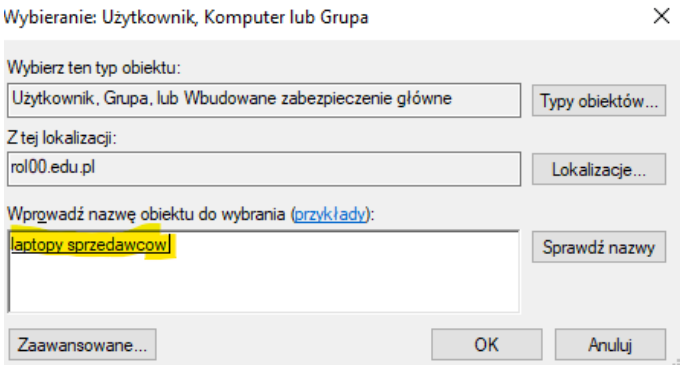


W konsoli Group Policy Management (Zarządzanie zasadami grupy) należy zaznaczyć obiekt zasad grupy Konfiguracja laptopów sprzedawców w kontenerze Group Policy Objects (Obiekty zasad grupy). Na karcie Scope (Zakres) w sekcji Security Filtering (Filtrowanie zabezpieczeń) należy zaznaczyć grupę Authenticated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

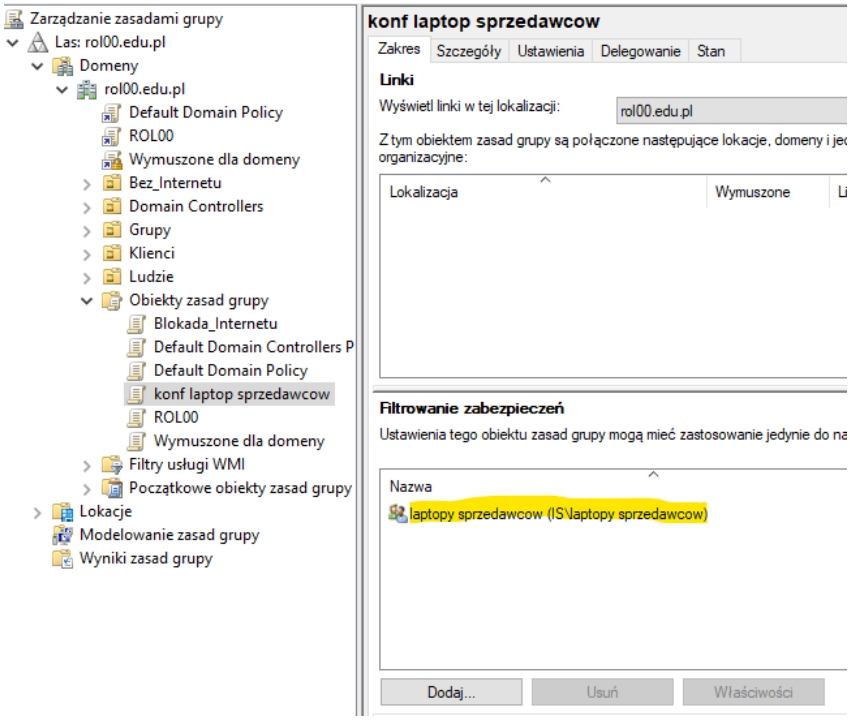


Kliknąć przycisk Add (Dodaj) W sekcji Security Filtering (Filtrowanie zabezpieczeń).

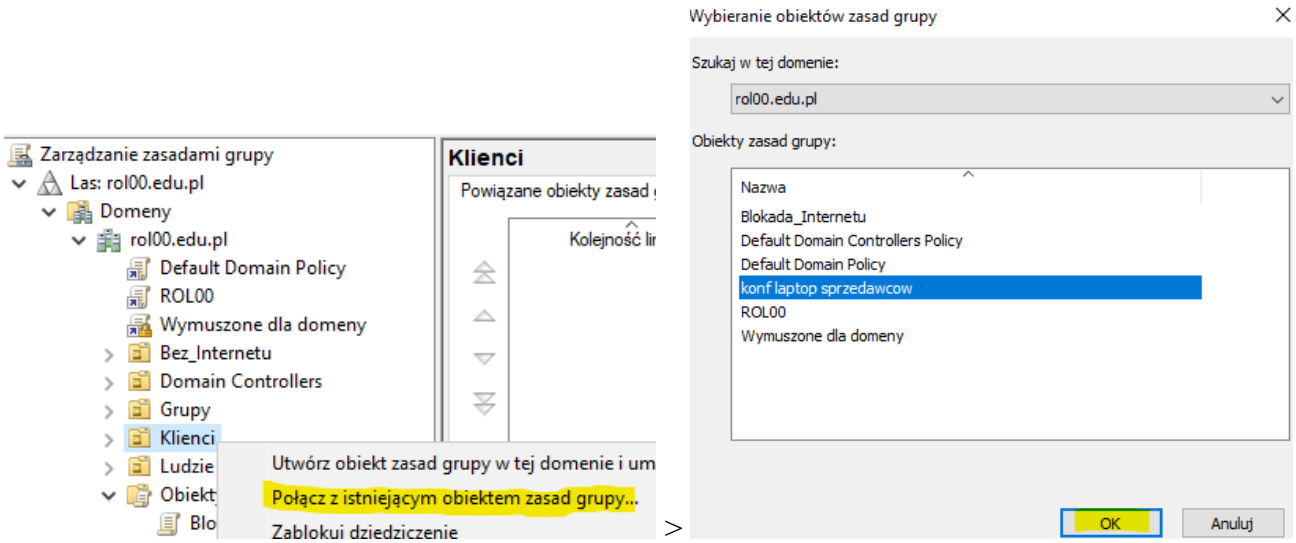
Wpisać nazwę grupy laptopy sprzedawcow i kliknąć OK.



Widok filtrowania zabezpieczeń – dodanie grupy „Laptopy sprzedawców”



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

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 wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.