Zasady grupy

Zasady grupy (ang. *Group Policies*) to obiekty zawierające zbiór ustawień konfiguracyjnych systemu. Zasady te obejmują ustawienia dla komputera oraz dla użytkownika. Można zaryzykować stwierdzenie, że dzięki zasadom grup można skonfigurować każdy element systemu *Windows XP* począwszy od instalacji oprogramowania przez konfiguracje środowiska użytkownika po zaawansowane opcje zabezpieczeń. Ustawienia zasad grup są przechowywane w obiektach *GPO* (ang. *Group Policy Object*).

Obiekty GPO mogą być lokalne dla komputera lub domenowe, przechowywane w usłudze *Active Directory*. Jeżeli komputer należy do grupy roboczej dotyczą go wyłącznie ustawienie lokalnych zasad grup, natomiast gdy należy do domeny, na konfigurację komputera wpływają również obiekty GPO stworzone przez administratora domeny.

Wszystkie zasady grupy zostały podzielone na dwie zasadnicze części *Konfiguracja komputera* i *Konfiguracja użytkownika*. Pierwsze ustawienia dotyczą parametrów komputera, które są ładowane podczas startu systemu jeszcze przed logowanie użytkownika. Drugie dotyczą ustawień specyficznych dla użytkownika i są ładowane w momencie logowania do systemu.

Zasady zabezpieczeń lokalnych

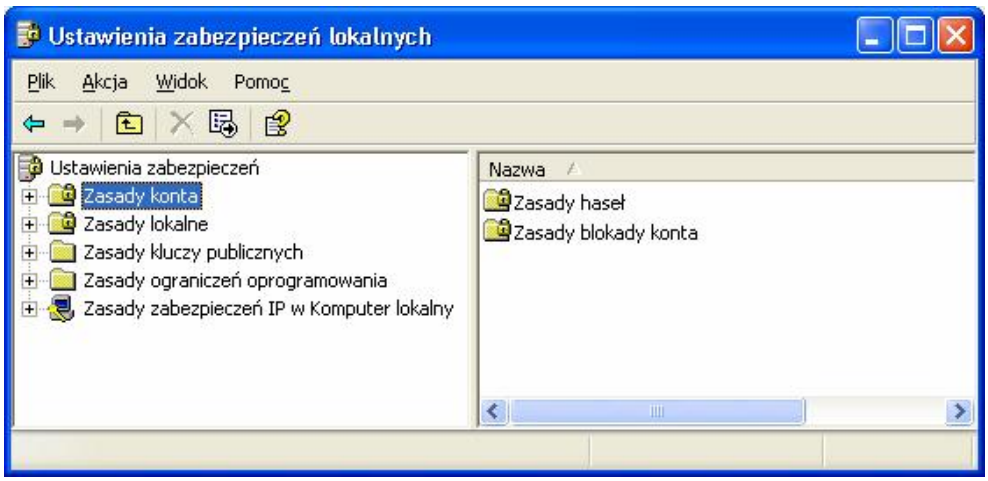
Windows XP zawiera szereg przystawek do konsoli MMC, które ułatwiają zarządzanie obiektami GPO. Jedną z nich jest przystawka Zasady grupy, którą wykorzystano do utworzenia predefiniowanej konsoli Zasady zabezpieczeń lokalnych (ang. *Local security policy*).

Predefiniowana konsola *Zasady zabezpieczeń lokalnych* zawiera przystawkę *Zasady grupy*, jednakże w celu uproszczenia jej obsługi zostały wyłączone niektóre rozszerzenia.

Za pomocą konsoli *Zasady zabezpieczeń lokalnych* użytkownik z uprawnieniami administratora może dowolnie skonfigurować zasady bezpieczeństwa komputera lokalnego. Zostały one podzielone na następujące grupy:

- *Zasady konta*
  Do których należą ustawienia blokowania konta oraz zasady haseł.
- *Zasady lokalne*
  Obejmujące zasady inspekcji, opcje zabezpieczeń i przypisywanie praw użytkownika.
- *Zasady kluczy publicznych*
  Ustawienia szyfrowania plików.
- *Zasady ograniczeń oprogramowania*

- *Zasady zabezpieczeń IP*



Konsola Zasady zabezpieczeń lokalnych

Każda z ww. grup zawiera listę ustawień, które można konfigurować, często lista ta jest bardzo obszerna. Poniżej zostały opisane najważniejsze ustawienia oraz ich wpływ na działanie systemu.

Ustawienia z grupy *Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady konta\Zasady haseł*

Podając powyższą lokalizację grupy oraz wszystkie kolejne lokalizacje złożyliśmy, iż do konfiguracji używana jest przystawka konsoli MMC *Zasady grupy*. Jeżeli wykorzystujesz predefiniowaną konsolę *Zasady zabezpieczeń lokalnych*, należy pominąć dwa pierwsze człony.

- *Hasło musi spełniać wymagania co do złożoności*
  Określa ono, czy hasła do kont użytkowników muszą spełniać wymagania co do złożoności znaków. Wymagania są następujące:
  - Nie mogą zawierać fragmentu lub całej nazwy konta użytkownika.
  - Muszą mieć długość minimum sześciu znaków.
  - Muszą zawierać znaki z trzech kategorii: Wielkie litery od A do Z, małe litery od a do z, 10 cyfr podstawowych od 0 do 9, znaki specjalne (;!,@#$*&).
- *Minimalny okres ważności hasła*
  Określa czas ustalany w dniach, jaki musi obowiązywać hasło użytkownika, aby mógł je zmienić. Ustawienie to doskonale uzupełnia się z ustawieniem *Wymuszaj tworzenie historii haseł* i zapobiega zmienianiu hasła kilkakrotnie raz za razem, aby wrócić do poprzedniego.
- *Maksymalny okres ważności hasła*
  Definiuje, ile dni użytkownik może używać hasła, zanim wygaśnie jego ważność.

- *Minimalna długość hasła*
  Ustawia minimalną liczbę znaków, jaką musi posiadać hasło.
- *Wymuszaj tworzenie historii haseł*
  Jeżeli jest włączone, system zapamiętuje określoną liczbę zmian hasła w celu zmuszenia użytkowników do używania różnych haseł.
- *Zapisz hasła dla wszystkich użytkowników w domenie, korzystając z szyfrowania odwracalnego*
  Niektóre protokoły do poprawnego działania wymagają, aby hasło było przechowywane w postaci zaszyfrowanej odwracalnym algorytmem.

Ustawienia z grupy *Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady konta\Zasady konta*

- *Próg blokady konta*
  Określa, po ilu nieudanych próbach logowania konto zostanie zablokowane.

- *Czas trwania blokady*
  Ustawia czas, po którym zablokowane konto automatycznie zostanie odblokowane.

- *Wyzeruj liczniki blokady konta po*
  Określa, po jakim czasie pomiędzy jednym nieudanym logowaniem a następnym, licznik blokady zostanie wyzerowany.

Ustawienia z grupy *Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Opcje zabezpieczeń*

- *Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika*
  Jeżeli ustawienie jest włączone, nazwa użytkownika, który ostatnio logował się do komputera, nie jest wyświetlana. Ustawienie znajduje zastosowanie w sytuacji, gdy nie jest stosowany ekran powitalny.
- *Logowanie interakcyjne: nie wymagaj naciśnięcia klawiszy CTRL+ALT+DEL*
  Gdy włączone, nie wymaga od użytkownika naciśnięcia ww. kombinacji klawiszy w celu przejścia do okna logowania. Ustawienie to jest domyślnie wyłączone na komputerach należących do domeny. Gdy komputer pracuje w grupie roboczej, jest włączone.
- *Logowanie interakcyjne: tekst komunikatu dla użytkowników próbujących się zalogować*
  Ustawienie pozwala na wpisanie treści komunikatu, który będzie się pojawiał po naciśnięciu kombinacji klawiszy *CTRL+ALT+DEL.*

  Aby komunikat się pojawił, musi być wyłączony ekran powitalny oraz wymagane naciśnięcie klawiszy *CTRL+ALT+DEL.*

- *Logowanie interakcyjne: tytuł komunikatu dla użytkowników próbujących się zalogować*
  Definiuje tytuł pojawiający się na górnej belce okna komunikatu.
- *Logowanie interakcyjne: monituj użytkownika o zmianę hasła przed jego wygaśnięciem*
  Ustala, ile dni przed wygaśnięciem hasła, użytkownik będzie informowany o potrzebie jego zmiany. Parametr ten powinien być ustawiony tak, aby ilość dni nie była większa niż wartość parametru Maksymalny okres ważności hasła pomniejszona o *Minimalny okres ważności hasła*.
- *Zamknięcie: zezwalaj na zamykanie systemu bez konieczności załogowania*
  Ustala, czy komputer system może być wyłączany przez użytkownika, który nie jest zalogowany. Jeżeli ustawienie jest włączone, na ekranie powitalnym lub w oknie logowania uaktywnia się przycisk *Zamknij system*.

Ustawienia z grupy *Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Przypisywanie praw użytkownika*

- *Logowanie lokalne*
  Zezwala wszystkim użytkownikom i grupom dodanym do ustawień tej zasady na logowanie lokalne do komputera.
- *Odmowa logowania lokalnego*
  Zabrania logowania lokalnego użytkownikom i grupom dopisanym do tej zasady. Ustawienie odmowy nadpisuje ustawienie przyzwolenia.
- *Uzyskiwanie dostępu do tego komputera z sieci*
  Zezwala na dostęp do komputera za pomocą sieci. Aby użytkownik mógł korzystać z udostępnionych zasobów, musi mieć nadane to uprawnienie na komputerze, który udostępnia wspomniane zasoby.
- *Odmowa dostępu do tego komputera z sieci*
  Odmawia dostępu do komputera przez sieć. Odmowa nadpisuje przyzwolenie.

Ustawienia z grupy *Konfiguracja użytkownika\Szablony administracyjne\System\Opcje klawiszy CTRL+ALT+DEL*

- *Usuń Menedżera zadań*
  Zabrania użytkownikom uruchamiania programu *Menedżer zadań* (*taskmgr.exe*).
- *Usuń opcję zablokuj komputer*
  Zapobiega blokowaniu systemu przez komputer.
- *Usuń opcję Zmień hasło*
  Uniemożliwia użytkownikom zmianę swoich haseł do systemu *Windows*. Blokuje przycisk Zmień hasło.
- *Usuń wylosowywanie*
  Blokuje możliwość wylogowywania się użytkownika.

To tylko niektóre ustawienia zasad bezpieczeństwa. Lista ustawień jest znacznie dłuższa, lecz niepotrzebne jest dokładne omawianie wszystkich parametrów.

Modyfikowanie zasad zabezpieczeń

Każdą zasadę zabezpieczeń można zmodyfikować, należy jednak przy tym pamiętać, że nieprzemyślana modyfikacja może mieć negatywny wpływ na działanie systemu. Dobrą praktyką jest modyfikowanie zasad na komputerze testowym, zanim zostaną one wprowadzone na komputery pracujące w środowisku produkcyjnym. Aby ustrzec się przed nieoczekiwanymi problemami, zaleca się postępowanie w następujący sposób:

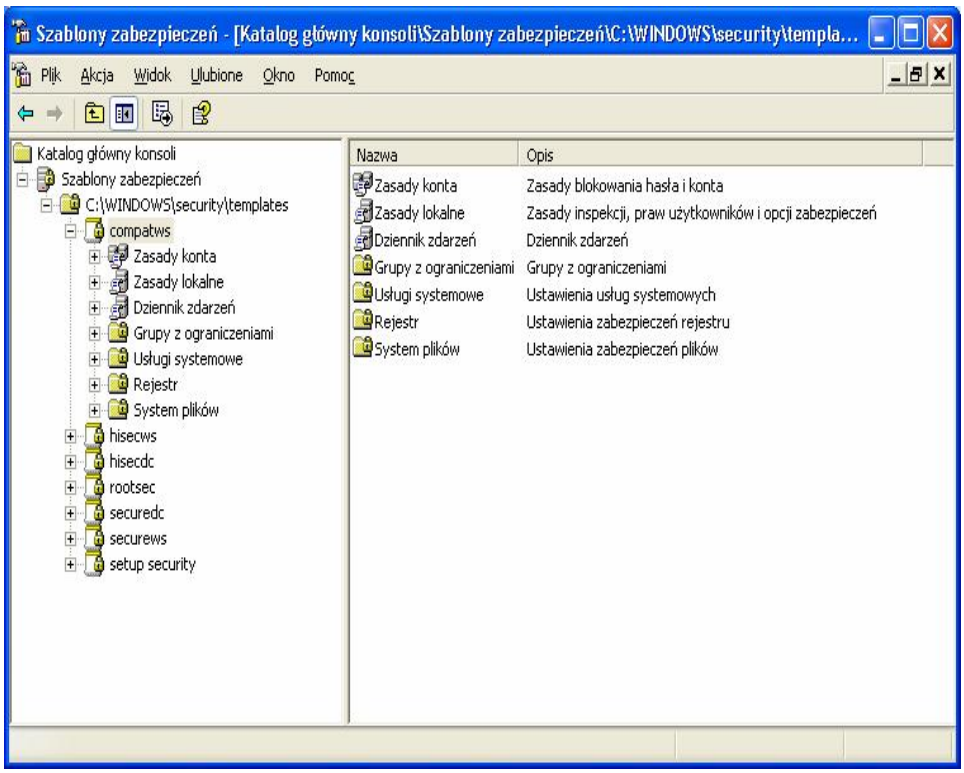
1. Zainstaluj na komputerze system *Windows XP* w identycznej konfiguracji jak w środowisku produkcyjnym.
2. Modyfikuj ustawienia zasad pojedynczo. Pozwoli to na szybki powrót do sytuacji z przed modyfikacji.
3. Po każdej zmianie testuj ustawienia.
4. Dopiero gdy wszystko zostało sprawdzone i przetestowane, powinno nastąpić wprowadzenie nowych zasad na pozostałe komputery.

Aby zmodyfikować ustawienia zasad:

1. Otwórz odpowiednią konsolę np. *Zasady zabezpieczeń lokalnych.*
2. Prawym przyciskiem myszy kliknij na ustawienie, które chcesz modyfikować i wybierz z menu podręcznego *Właściwości.*
3. Ustaw parametry zasady. W większości przypadków będą to dwie opcje *Włącz* lub *Wyłącz*, jednakże niektóre zasady wymagają dodatkowych parametrów liczbowych lub tekstowych.
4. Kliknij *OK*, aby zatwierdzić zmiany.

Szablony zabezpieczeń

Ponieważ bardzo duża ilość ustawień konfiguracyjnych obiektów GPO może sprawiać trudności podczas doboru właściwych wartości dla poszczególnych ustawień, system *Windows XP* został wyposażony w kilka gotowych *szablonów zabezpieczeń* oraz narzędzia służące do ich implementacji w systemie. *Szablony zabezpieczeń* to predefiniowane ustawienia, które występują w postaci plików z rozszerzeniem *.inf* i umieszczone są w następującym folderze *%systemroot%\security\templates*. Można je wykorzystywać podczas konfigurowania zasad bezpieczeństwa komputera. Aby było to możliwe, należy stworzyć konsolę zawierającą przystawkę Szablony zabezpieczeń. W konsoli tej zostaną wyświetlone w uporządkowany sposób wszystkie szablony oraz ich ustawienia.



Konsola z przystawką Szablony zabezpieczeń

Poziomy zabezpieczeń

Predefiniowane szablony zabezpieczeń różnią się poziomem bezpieczeństwa, jaki zapewniają zawarte w nich ustawienia. Zostały one tak przygotowane, aby odpowiadały najczęstszym wymaganiom. Zawierają cztery poziomy zabezpieczeń: *podstawowy (setup), zgodny (compatible), bezpieczny (secure)* oraz *wysoki (high).*

Katalog *%systemroot%\security\templates* zawiera szablony, które są przeznaczone dla serwerów i stacji roboczych oraz dla kontrolerów domeny. Istotne jest, aby konfigurując *Windows XP*, używać szablonów przeznaczonych dla stacji roboczych. Rozróżnić można je dzięki ostatnim dwóm znakom w nazwie, są to litery *ws*.

- *Poziom podstawowy*
  Jest to standardowy poziom zabezpieczeń, jaki jest stosowany podczas instalacji systemu *Windows XP*.
  Nazwa szablonu *setup security.*
- *Poziom zgodny*
  Wyższy poziom zabezpieczeń zapewniający działanie wszystkich aplikacji biurowych.
  Nazwa szablonu *compatws.*
- *Poziom bezpieczny*
  Określa konfigurację wysokiego poziomu zabezpieczeń, lecz jego wykorzystanie

nie daje pewności, że wszystkie aplikacje i (lub) ich funkcje będą działać prawidłowo.
Nazwa szablonu: *securews.*

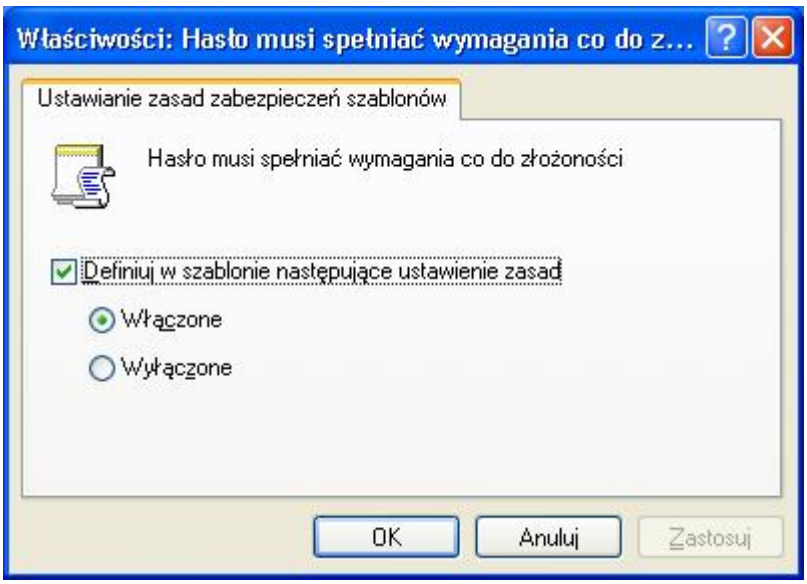
- *Poziom wysoki*
  Zapewnia maksymalny poziom zabezpieczeń systemu *Windows XP*, który został osiągnięty kosztem poprawnej pracy aplikacji.
  Nazwa szablonu: *hisecws.*

Modyfikowanie szablonów

Predefiniowane szablony należy traktować jako punkt wyjścia do dalszej konfiguracji. Każdy z predefiniowanych szablonów można zmodyfikować i zapisać jako nowy szablon. Aby to wykonać:

1. Otwórz konsolę zawierającą przystawkę *Szablony zabezpieczeń.*
2. Wybierz szablon, który chcesz modyfikować następnie rozwiń jego strukturę w drzewie konsoli.
3. Zmodyfikuj wybrane ustawienia.

Podczas modyfikacji ustawień użytkownik ma zwykle trzy możliwości. Jeżeli pole wyboru *Definiuj w szablonie następujące ustawienie zasad* jest niezaznaczone, dane ustawienie będzie niezdefiniowane, co oznacza, że ustawienie to nie zmienia nic w konfiguracji komputera i pozostawia ją bez zmian. W przeciwnym przypadku należy dodatkowo wybrać jedną z dwóch opcji *Włączone* lub *Wyłączone.*



Modyfikowanie zasady zabezpieczeń

Opisana powyżej procedura modyfikacji ustawień nie dotyczy wszystkich zasad. Niektóre zasady wymagają dodatkowej konfiguracji np. wpisania ilości dni lub innych parametrów typu liczbowego lub tekstowego.

4. Kliknij prawym klawiszem myszy na nazwę szablonu i z menu podręcznego wybierz *Zapisz jako…*
5. Wskaż lokalizację oraz nazwę dla nowego szablonu.
6. Kliknij *Zapisz.*

Po zapisaniu na liście dostępnych szablonów pojawi się nowa pozycja.