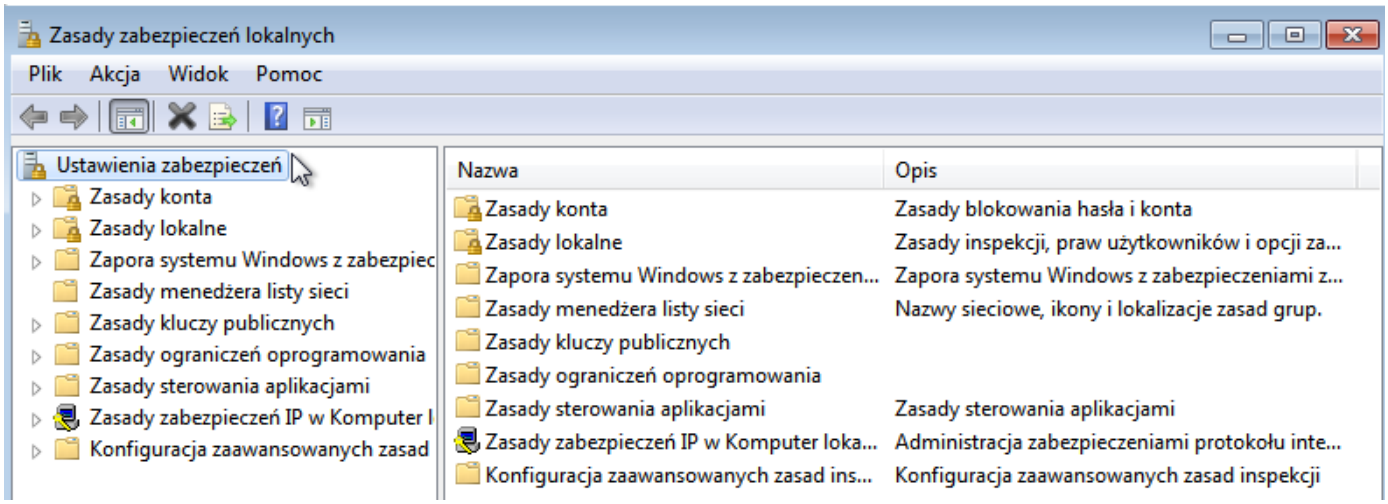
Zasady zabezpieczeń lokalnych.

Wykonaj poniższe zadania i notatkę na temat wykonanych poleceń.

1. Konfiguracja zasad bezpieczeństwa komputera lokalnego.

Skonfiguruj zasady bezpieczeństwa komputera lokalnego za pomocą konsoli Zasady zabezpieczeń lokalnych jako użytkownik z uprawnieniami administratora.

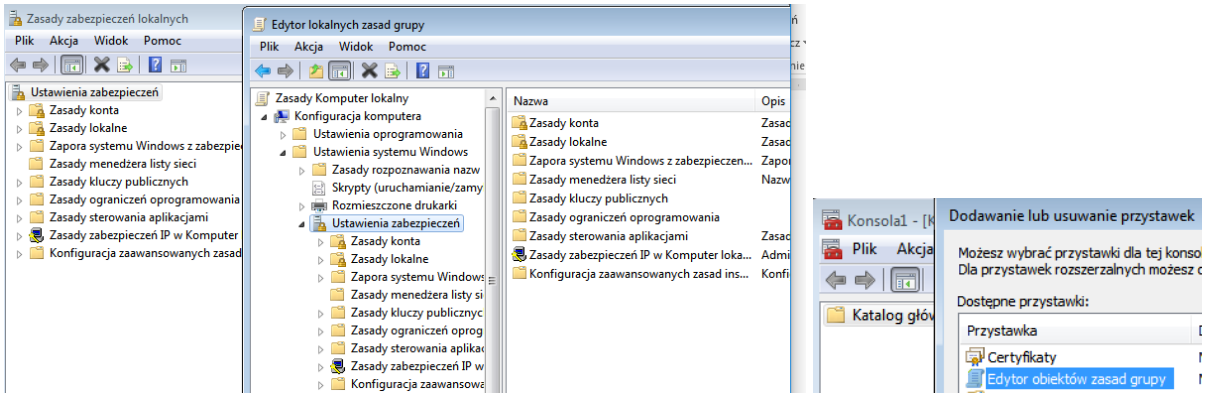
Zasady zabezpieczeń lokalnych zostały podzielone na grupy.



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

a) Ustawienia z grupy - k*onfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady konta\Zasady haseł*

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



- Hasło musi spełniać wymagania co do złożoności - włącz

  Określa, 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 – pozostaw 2 dni.

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 zmianie hasła kilkakrotnie raz za razem, aby wrócić do poprzedniego.

- Maksymalny okres ważności hasła - Definiuje, ile dni użytkownik może używać hasła, zanim wygaśnie jego ważność – pozostaw 32 dni.
- Minimalna długość hasła - Ustawia minimalną liczbę znaków, jaką musi posiadać hasło – pozostaw 8.
- Wymuszaj tworzenie historii haseł - Jeżeli jest włączone, system zapamiętuje określoną liczbę zmian hasła w celu zmuszenia użytkowników do używania różnych haseł. – pozostaw 2
- 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.

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

- Próg blokady konta - Określa, po ilu nieudanych próbach logowania konto zostanie zablokowane – pozostaw 5, zaakceptuj odpowiedz na pytanie.
- 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.

c) 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 - pozostaw Włączone.
- 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 zalogowania - 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*.

d) 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 - pozostaw użytkownika Gość.
- 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 – pozostaw użytkownika Gość.
- Zmień czas systemowy – pozostaw dodaną grupę Użytkownicy uwierzytelnieni.

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

- Usuń Menedżera zadań - Zabrania użytkownikom uruchamiania programu *Menedżer zadań* (*taskmgr.exe*) – pozostaw Włączone.

- Usuń opcję zablokuj komputer - Zapobiega blokowaniu systemu przez komputer - pozostaw Włączone.
- Usuń opcję Zmień hasło - Uniemożliwia użytkownikom zmianę swoich haseł do systemu *Windows*. Blokuje przycisk Zmień hasło.
- Usuń wylogowywanie - Blokuje możliwość wylogowywania się użytkownika.

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

f) Zaktualizuj wprowadzone zmian w zasadach zabezpieczeń grup, użyj polecenia: gpupdate /force

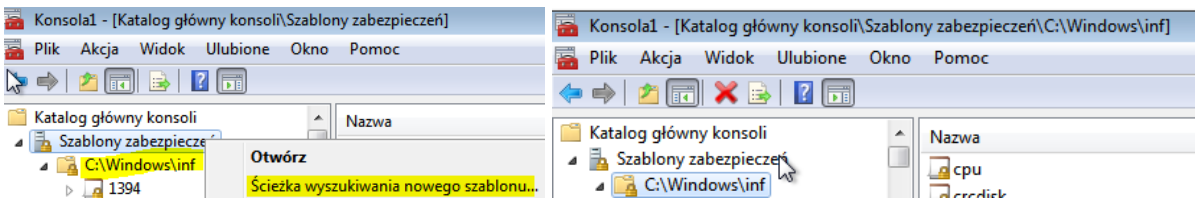
Modyfikowanie zasad zabezpieczeń.

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:

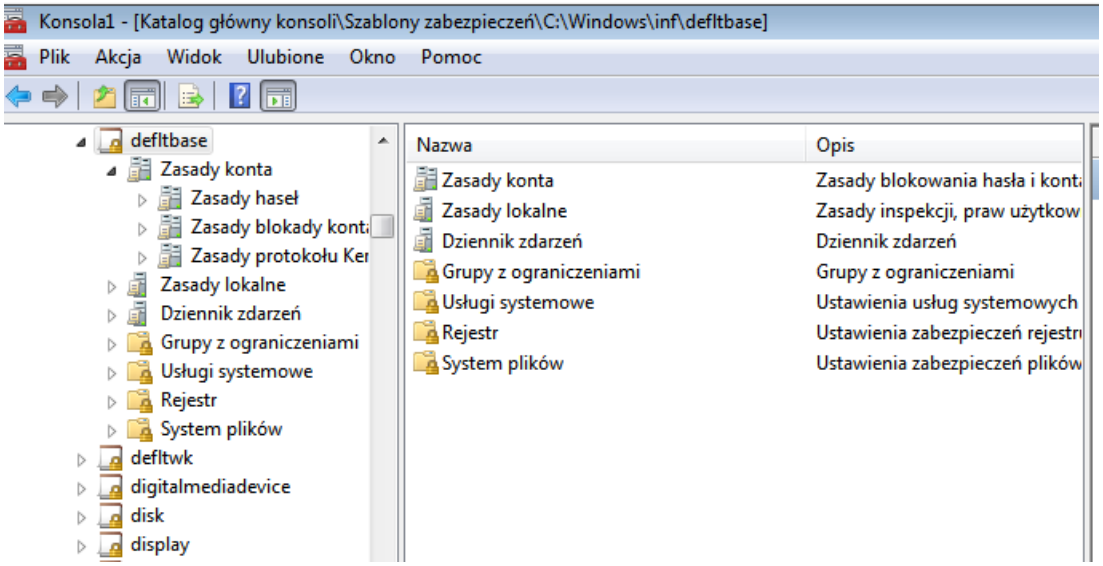
1. Modyfikuj ustawienia zasad pojedynczo. Pozwoli to na szybki powrót do sytuacji z przed modyfikacji.
2. Po każdej zmianie testuj ustawienia.
3. Dopiero gdy wszystko zostało sprawdzone i przetestowane, powinno nastąpić wprowadzenie nowych zasad na pozostałe komputery.

2. Szablony zabezpieczeń.

Ponieważ bardzo duża ilość ustawień konfiguracyjnych obiektów GPO może sprawiać trudności podczas doboru właściwych wartości dla poszczególnych ustawień, system *Windows* został wyposażony w gotowe szablony *zabezpieczeń* oraz narzędzia służące do ich implementacji w systemie. *Szablon zabezpieczeń* to predefiniowane ustawienia, które występują w postaci plików z rozszerzeniem *.inf* i umieszczony jest w folderze *%systemroot%*\inf\ przykładowy plik Defltbase.inf - domyślny szablon zabezpieczeń używany przez system Windows. Można je wykorzystywać podczas konfigurowania zasad bezpieczeństwa komputera.



Aby było to możliwe, utwórz konsolę zawierającą przystawkę Szablony zabezpieczeń. W konsoli tej zostaną wyświetlone w uporządkowany sposób wszystkie szablony oraz ich ustawienia.



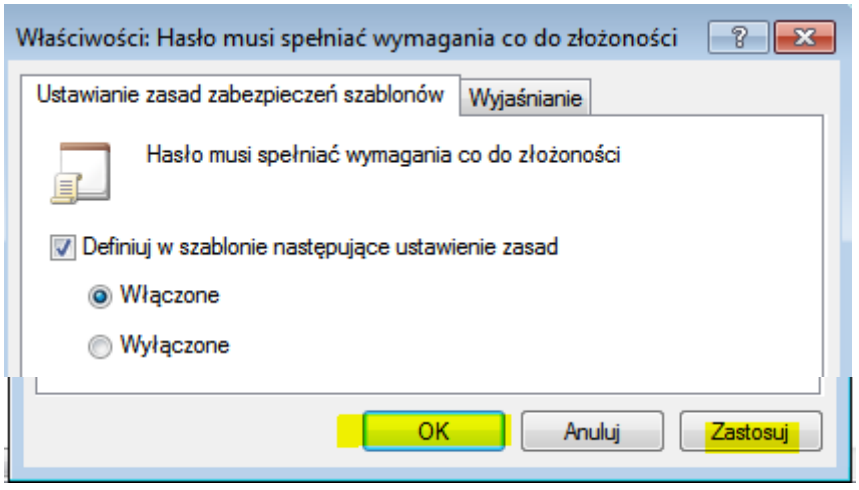
3. Modyfikowanie szablonów.

Predefiniowane szablony należy traktować jako punkt wyjścia do dalszej konfiguracji.

Każdy z predefiniowanych szablonów zmodyfikuj i zapisz 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.



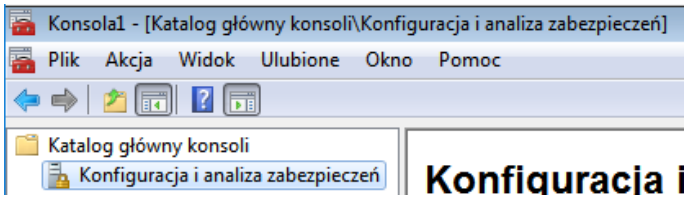
Opisana powyżej procedura modyfikacji ustawień nie dotyczy wszystkich zasad. Niektóre zasady wymagają dodatkowej konfiguracji np. wpisania ilości dni lub innych parametrów typu liczbowego lub tekstowego.

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

Po zapisaniu na liście dostępnych szablonów pojawi się nowa pozycja.

4. Konfiguracja i analiza zabezpieczeń.

Kolejnym narzędziem, które oferuje duże możliwości konfiguracji zabezpieczeń systemu jest przystawka Konfiguracja i analiza zabezpieczeń.



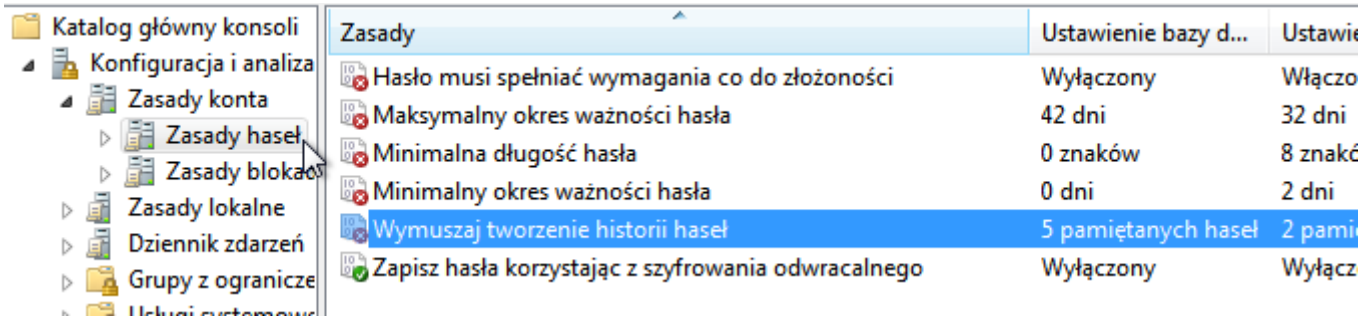
Jest to narzędzie służące do porównywania aktualnych ustawień komputera z tymi, które są zawarte w szablonie bez wpływu na bieżącą konfigurację. Narzędzie to jest szczególnie przydatne podczas tworzenia i testowania nowych ustawień i (lub) szablonów. Aby skorzystać z Konfiguracji i analizy zabezpieczeń, należy dodać do konsoli odpowiednią przystawkę (można wykorzystać konsolę stworzoną do konfiguracji i przeglądania szablonów).
Analiza polega na porównaniu ustawień komputera lokalnego z alternatywną konfiguracją pobraną z szablonu i przechowywaną w osobnej utworzonej specjalnie do porównania *bazie (plik .sdb).*

Aby porównać dwie konfiguracje zabezpieczeń:

1. Dodaj do konsoli przystawkę Konfiguracja i analiza zabezpieczeń.
2. Kliknij prawym przyciskiem myszy na przystawkę i wybierz z menu podręcznego Otwieranie bazy danych…
3. Wskaż domyślną lokalizację, w której chcesz utworzyć plik bazy oraz nazwę bazy nowy.
4. Kliknij przycisk Otwórz.
5. W oknie Importuj szablon wybierz z C: Windows\inf\ szablon nowy, który zostanie zaimportowany do bazy. Jest to szablon, z którym będzie porównywana aktualna konfiguracja komputera.
6. Kliknij Otwórz.
7. Ponownie kliknij prawym przyciskiem myszy na przystawkę Konfiguracja i analiza zabezpieczeń i wybierz z menu podręcznego Analizuj komputer teraz…
8. W oknie Wykonywanie analizy wskaż lokalizację, w której będzie zapisany plik dziennika błędów. Plik ten może być potrzebny w późniejszej analizie.

9. Kliknij OK.

Rozpocznie się porównywanie dwóch konfiguracji, na ekranie będzie widoczne okno przedstawiające aktualnie analizowane elementy oraz stan zaawansowania operacji. Po zakończeniu procesu analizy sprawdź jej wyniki, przeglądając ustawienia w oknie szczegółów.



Pozostaw tak jak na rysunku powyżej, zapisz w zeszycie co to oznacz.

Okno szczegółów zawiera trzy kolumny: Zasady – w której znajduje się nazwa analizowanej zasady, Ustawienie bazy danych - gdzie wyświetlane jest ustawienie pobrane z bazy *.sdb* oraz Ustawienie komputera - zawierające parametry pobrane z komputera lokalnego. Przed nazwą każdej zasady umieszczona jest ikona, która przedstawia wynik analizy. Jeżeli ikona zawiera na czerwonym tle znak *x*, oznacza to, iż ustawienie komputera jest mniej bezpieczne niż ustawienie proponowane w szablonie.

W przypadku gdy ikona zawiera zielony haczyk na białym tle, oznacza to, że ustawienia bazy i komputera są identyczne. Ikona ze znakiem zapytania informuje o tym, że nie została przeprowadzona analiza tej zasady, gdyż w ustawieniach komputera nie została ona w ogóle określona i program nie miał możliwości porównania.

Jeżeli ikona nie zawiera żadnych dodatkowych symboli, oznacza to, że zasada nie została zdefiniowana w bazie i nie można było zrobić porównania.

Jeżeli ustawienia proponowane nie są odpowiednie, można je zmodyfikować, klękając na wybraną zasadę prawym klawiszem myszy i wybierając z menu podręcznego Właściwości.

Wprowadzane zmiany są zapisywane w bazie. Aby sprawdzić, jak wypada porównanie zmienionych zasad z zasadami komputera lokalnego, należy ponownie uruchomić analizę.

5. Konfigurowanie zabezpieczeń.

Ustawienia odpowiadają wymaganiom bezpieczeństwa, należy je **zastosować na komputerze lokalnym**. Aby to zrobić:

1. Kliknij prawym przyciskiem myszy na przystawkę Konfiguracja i analiza zabezpieczeń.
2. Z menu podręcznego wybierz Konfiguruj komputer teraz …
3. W oknie Konfigurowanie systemu wskaż lokalizację dla pliku dziennika i zatwierdź przyciskiem OK.

Nastąpi przekonfigurowanie ustawień komputera zgodnie z ustawieniami w bazie *.sdb*.

Zastosuj zdefiniowane ustawienia na innych komputerach (stosowane np. gdy w sieci jest wprowadzany standard zabezpieczeń dla wszystkich stacji roboczych, by nie analizować i zmieniać ustawień ręcznie na każdej stacji od początku) wykorzystaj narzędzie **Konfiguracja i analiza zabezpieczeń do wyeksportowania nowego szablonu**. Aby to zrobić:

1. Zmodyfikuj ustawienia w bazie danych tak, aby odpowiadały Twoim wymaganiom.
2. Kliknij prawym przyciskiem myszy na Konfiguracja i analiza zabezpieczeń.
3. Wybierz z menu podręcznego Eksportuj szablon …
4. Wskaż nazwę nowy1 i domyślną lokalizację dla pliku szablonu, który zostanie utworzony.
5. Kliknij przycisk Zapisz.

Został zapisany **nowy plik szablonu,** który można **wykorzystać na innych komputerach w celu ich przekonfigurowania**. Aby to zrobić, należy wykorzystać narzędzie Konfiguracja i analiza zabezpieczeń, a stworzony szablon wykorzystać jako źródło ustawień dla bazy danych lub skorzystać z Zasady zabezpieczeń lokalnych w celu załadowania szablonu. Aby to zrobić:

1. Uruchom konsolę Zasady zabezpieczeń lokalnych.
2. Kliknij prawym przyciskiem myszy na Ustawienia zabezpieczeń.
3. Wybierz z menu podręcznego Importuj zasady …
4. Wskaż plik szablonu nowy1, który chcesz importować.
5. Kliknij Otwórz.
6. Sprawdź, czy zostały załadowane do ustawień lokalnego komputera ustawienia pobrane z szablonu.

Uwaga teleinformatycy nie wykonują 6. Zarządzanie zasadami zabezpieczeń z Wiersza polecenia

6. Zarządzanie zasadami zabezpieczeń z Wiersza polecenia

Zarządzanie zasadami zabezpieczeń można prowadzić także z poziomu *Wiersza polecenia*.
Operacje wykonywane w wierszu polecenia umożliwiają konfigurację zabezpieczeń przy wykorzystaniu skryptów. Polecenie, które jest wykorzystywane do zarządzania zabezpieczeniami to *secedit.exe*.
polecenie posiada kilka funkcji, które nie są dostępne z poziomu graficznego interfejsu użytkownika. Jedną z takich funkcji jest manualne odświeżanie zasad zabezpieczeń.

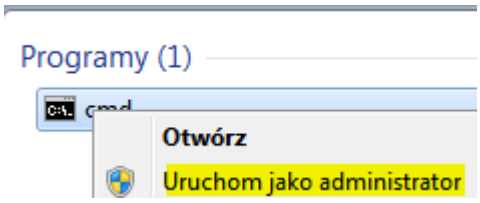
Za pomocą polecenia *secedit.exe* wykonać pięć operacji:

- Przełączniki */analyze*, */configure* oraz */export* odpowiadają tym samym operacjom, które są dostępne w programie Konfiguracja i analiza zabezpieczeń. Wymagają one wskazania przełącznikiem */db* bazy, która będzie wykorzystywana podczas pracy polecenia *secedit.*

Przełącznikiem */cfg* można wskazać szablon przeznaczony do importu. Obsługiwany jest również specjalny tryb pracy, który pomija wyświetlanie danych wyjściowych na ekranie oraz zapisywanie ich do pliku dziennika. Możliwe jest jednak przeglądanie wyników działania polecenia narzędziem Konfiguracja i analiza zabezpieczeń.

- Gdy korzystamy z przełącznika */configure*, możliwe jest użycie przełącznika */overwrite*, który powoduje, że szablon wskazany przełącznikiem */cfg* nadpisuje ustawienia, które znajdują się w pliku bazy danych. Jeżeli nie zostanie wykorzystany przełącznik */overwrite*, importowany szablon domyślnie dopisuje się do bazy. Przełącznik */areas* określa obszary ustawień, które będą podlegały zmianą konfiguracyjnym.

Uruchom cmd jako administrator



a) Zrestartuj wszystkie uprawnień zabezpieczeń do domyślnych? (System Windows 7)

secedit /configure /cfg %windir%\inf\defltbase.inf /db defltbase.sdb /verbose

```
C:\Windows\system32>secedit /configure /cfg C:\Windows\inf\defltbase.inf /db def
ltbase.sdb /verbose

Zadanie zostało ukończone. Podczas tej operacji wystąpiły ostrzeżenia dotyczące
niektórych atrybutów. Można zignorować ostrzeżenie.
Szczegółowe informacje można znaleźć w dzienniku %windir%\security\logs\scesrv.l
og.
```

b) Wykonaj następujące polecenie

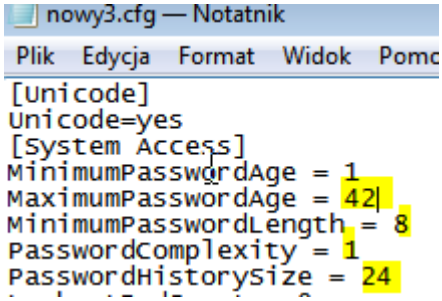
secedit /configure /cfg C:\Windows\inf\nowy1.inf /db nowy2.sdb /verbose

```
C:\Windows\system32>secedit /configure /cfg C:\Windows\inf\nowy1.inf /db nowy2.s
db /verbose

Zadanie zostało ukończone. Podczas tej operacji wystąpiły ostrzeżenia dotyczące
niektórych atrybutów. Można zignorować ostrzeżenie.
Szczegółowe informacje można znaleźć w dzienniku %windir%\security\logs\scesrv.l
og.
```

c) Wykonaj następujące polecenie secedit.exe /export /cfg C:\nowy3.cfg

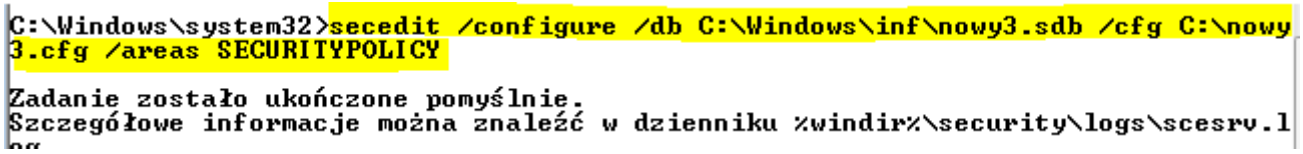
```
C:\Windows\system32>secedit /export /cfg C:\nowy3.cfg

Zadanie zostało ukończone pomyślnie.
Szczegółowe informacje można znaleźć w dzienniku %windir%\security\logs\scesrv.l
```

d) Edytuj odpowiednie zasady, jak pokazano i zmień jak poniżej.



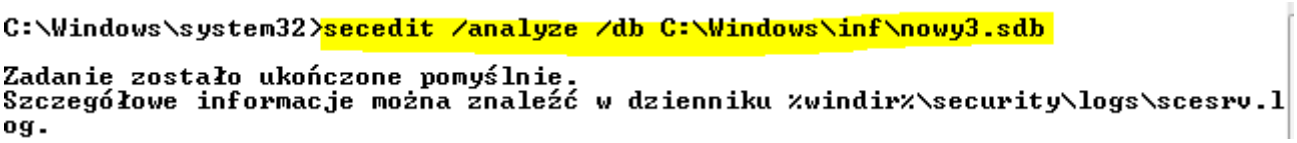
e) Po zakończeniu zapisz zmiany. Aby załadować edytowany plik jako nową konfigurację zasad, użyj następującego polecenia:

secedit.exe /configure /db C:\Windows\inf\nowy3.sdb /cfg C:\nowy3.cfg /areas SECURITYPOLICY

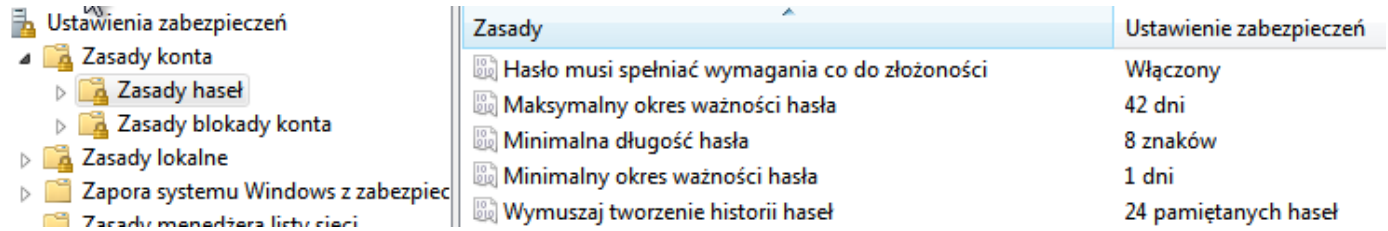


f) Wykonaj analizowanie bieżących ustawień systemu względem ustawień podstawowych przechowywanych w bazie danych:

secedit.exe /analyze /db C:\Windows\inf\nowy3.sdb

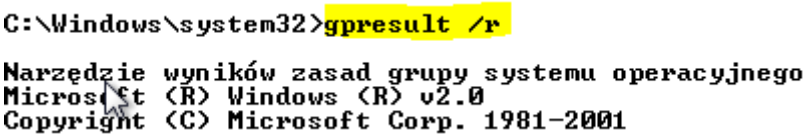


g) W celu weryfikacji otwórz Zasady zabezpieczeń lokalnych i sprawdz ustawienia zasad:



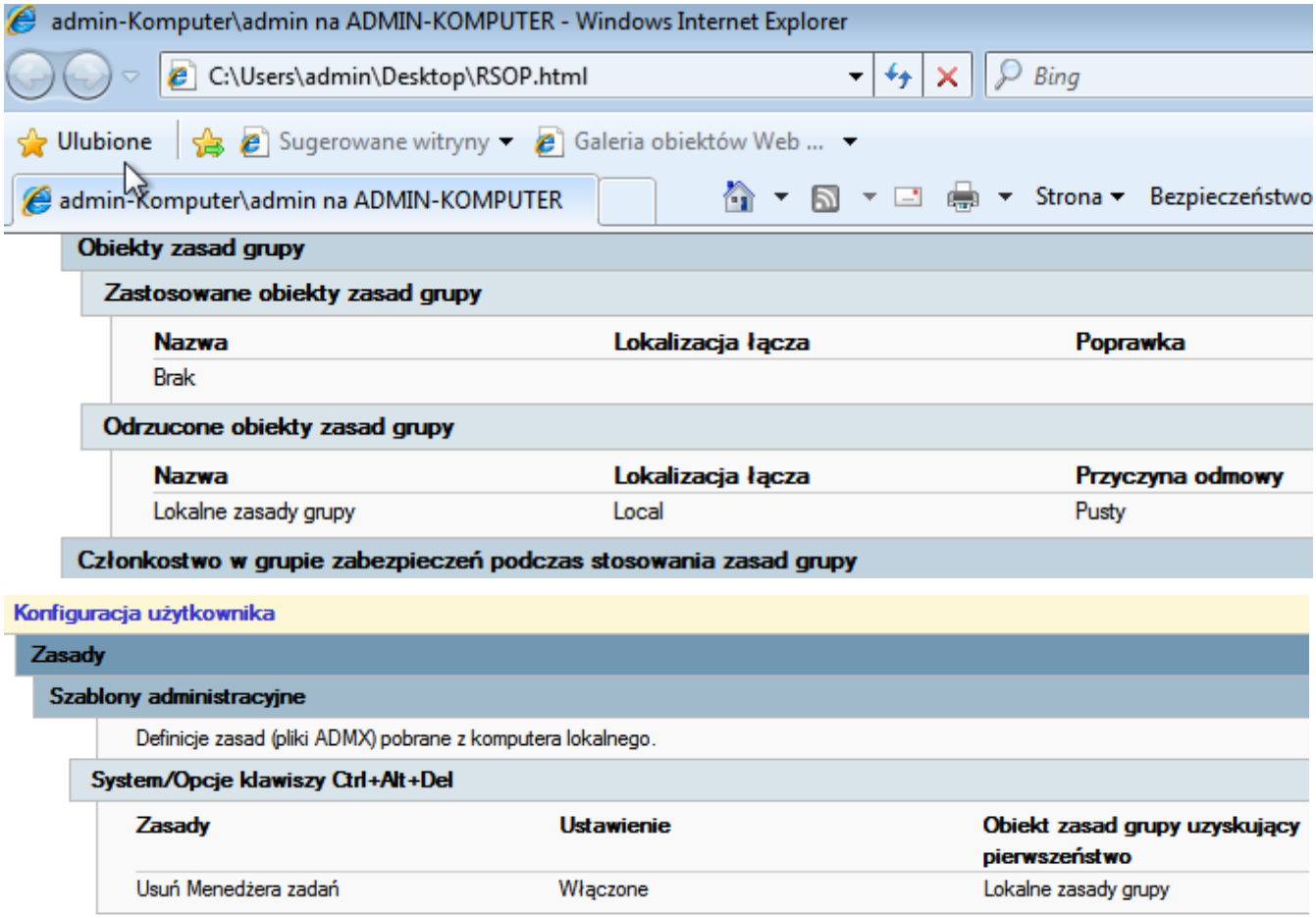
h) Do zaktualizowania wprowadzonych zmian w zasadach zabezpieczeń grup użyj polecenia:
gpupdate /force

i) Wykonaj polecenie gpresult /r i zinterpretuj uzyskane informacje.



j) Wykonaj polecenie gpresult /h:”%USERPROFILE%\Desktop\RSOP.html” i zinterpretuj uzyskane informacje.

```
C:\Windows\system32>gpresult /h:"%USERPROFILE%\Desktop\RSOP.html"
```



k) Utwórz w systemie konto nowego użytkownika, skonfiguruj tak jego prawa, aby nie mógł zalogować się do systemu.

l) Czy da się zmienić hasło użytkownika na takie które nie spełnia warunków hasła, jaki będzie tego efekt?