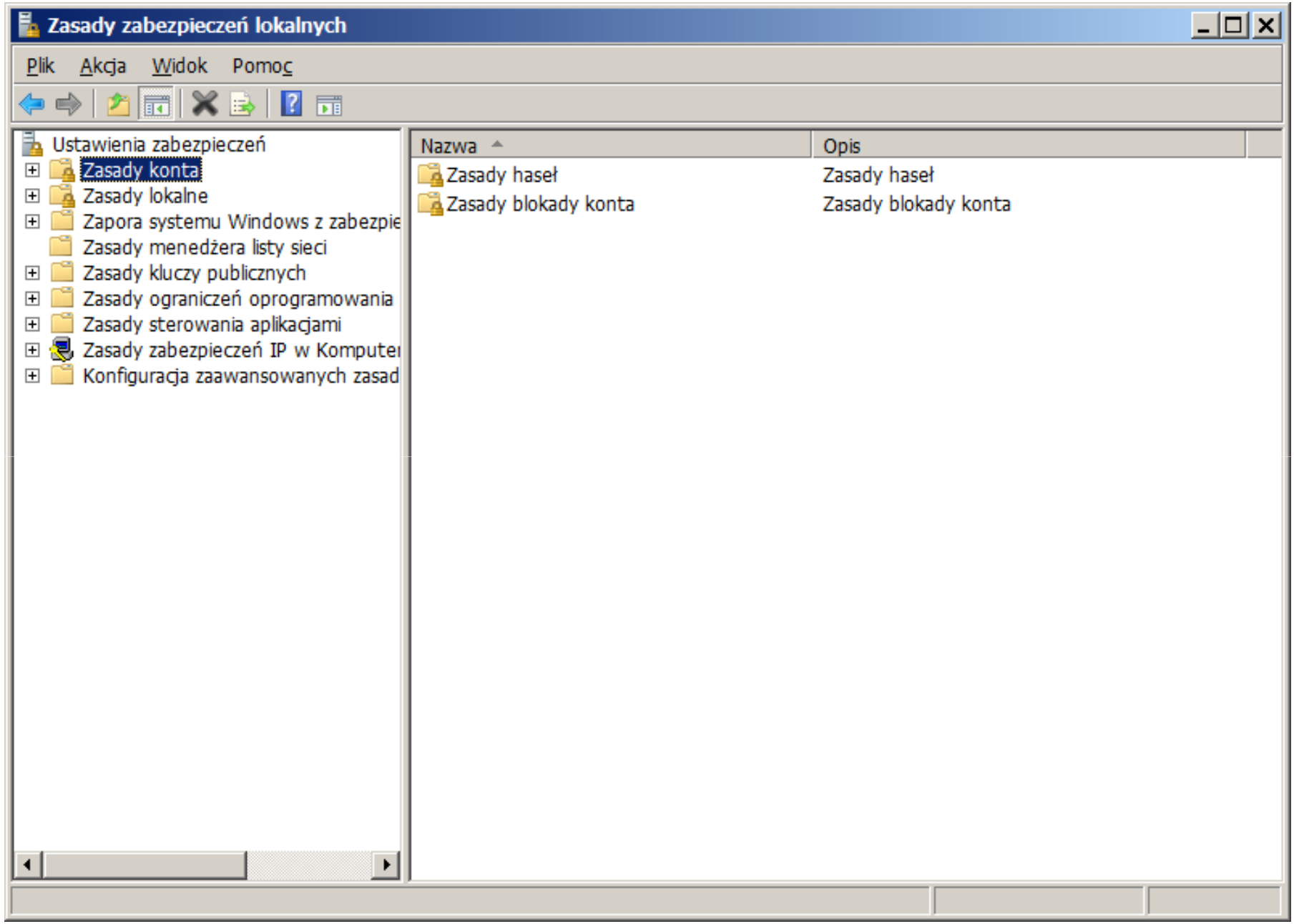
Zasady zabezpieczeń lokalnych

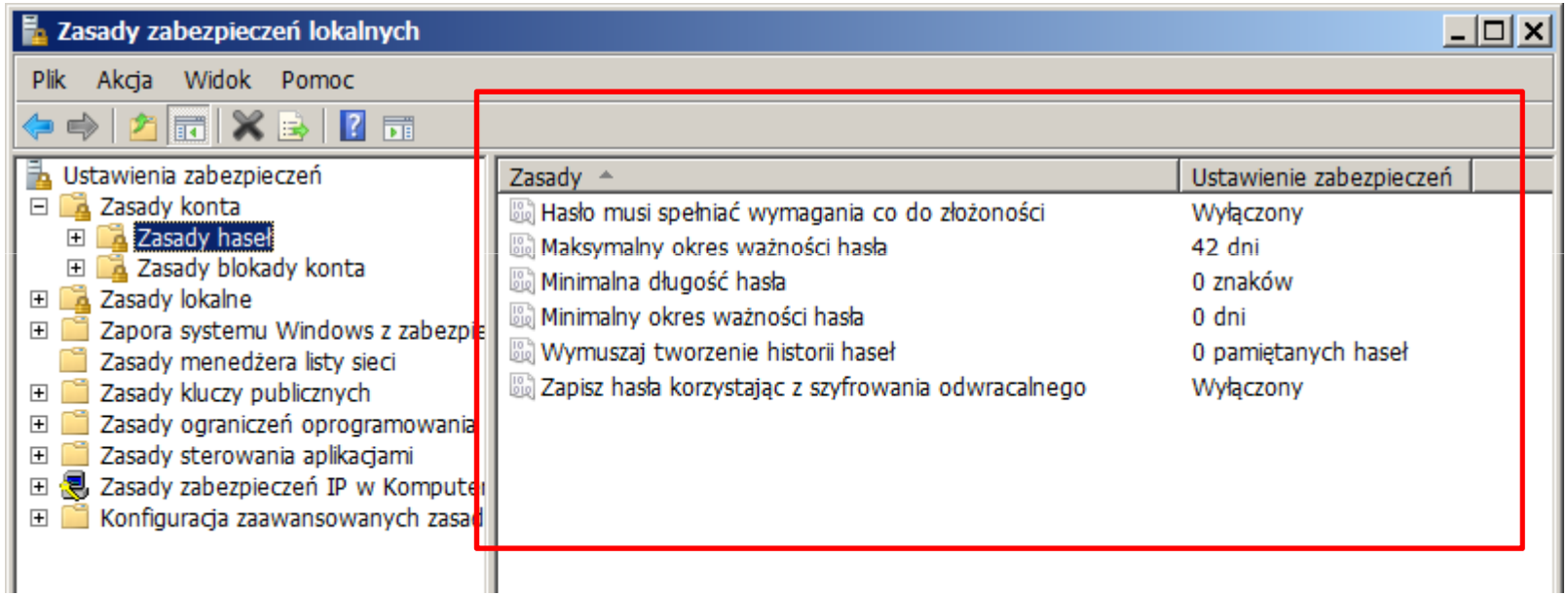
- Aplikację **Zasady zabezpieczeń lokalnych** uruchamiamy w **Panelu sterowania** wybierając **Narzędzia administracyjne** i **Zasady zabezpieczeń lokalnych**.
- Lub komendą **secpol.msc**
- Za jej pomocą użytkownik z uprawnieniami administratora może dowolnie skonfigurować zasady bezpieczeństwa lokalnego komputera.


Zasady zabezpieczeń lokalnych
Plik
Akcja
Widok
Pomoc
Ustawienia zabezpieczeń
Zasady konta
Zasady lokalne
Zapora systemu Windows z zabezpie
Zasady menedżera listy sieci
Zasady kluczy publicznych
Zasady ograniczeń oprogramowania
Zasady sterowania aplikacjami
Zasady zabezpieczeń IP w Komputer
Konfiguracja zaawansowanych zasad
Nazwa
Opis
Zasady haseł
Zasady haseł
Zasady blokady konta
Zasady blokady konta

- Zasady te podzielono na następujące grupy:
  - **Zasady konta** – do nich zalicza się ustawienia blokady kont oraz zasady haseł
  - **Zasady lokalne** – obejmują zasady inspekcji, opcje zabezpieczeń i ustawienia związane z przypisywaniem praw użytkownikom
  - **Zasady kluczy publicznych**, zawierające ustawienia dotyczące szyfrowania plików
  - **Zasady ograniczeń oprogramowania**, umożliwiające określenie programów, które można uruchamiać na komputerze
  - **Zasady zabezpieczeń IP** – pozwalają zabezpieczyć komunikację sieciową.

Ograniczenia dotyczące haseł użytkowników

- Dla użytkowników można wprowadzić różne ograniczenia związane z hasłami:



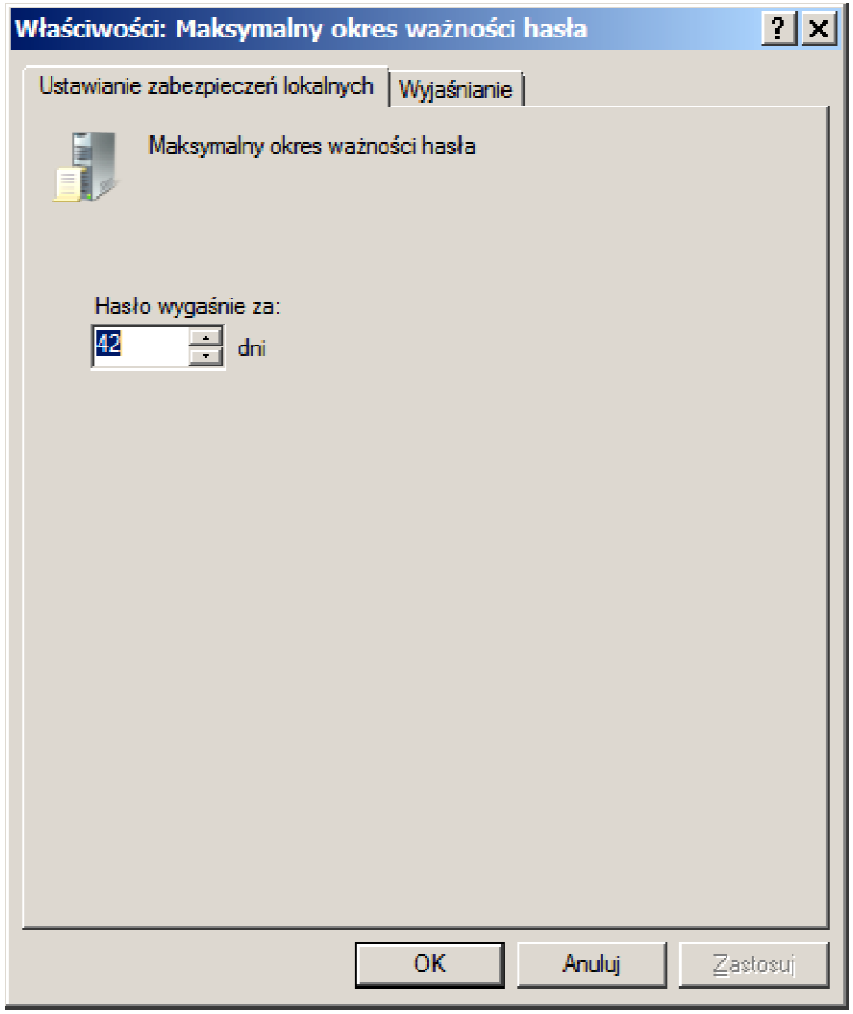
Domyślnie w systemie Windows wymagania złożoności haseł są wyłączone, należy je włączyć przed modyfikacją pozostałych opcji. Aby zmienić opcję należy ją dwukrotnie kliknąć i zmienić wartość.

Wymagania co do złożoności

- Włączenie tej opcji pozwala narzucić dodatkowe wymagania na złożoność hasła, np. minimalną długość, czy stosowanie silnych haseł.

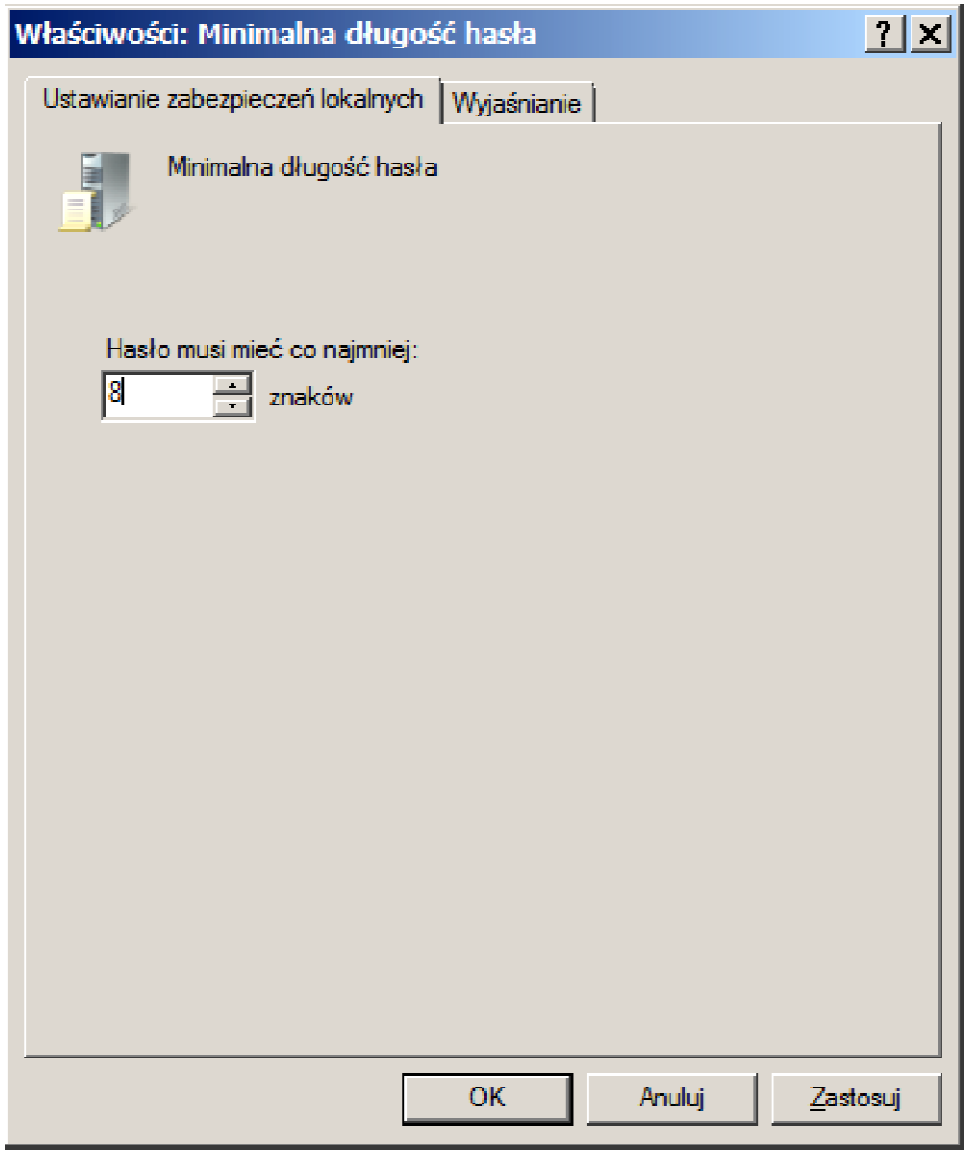
Maksymalny okres ważności hasła

- Maksymalny okres ważności hasła – co ile dni użytkownik musi zmienić hasło.



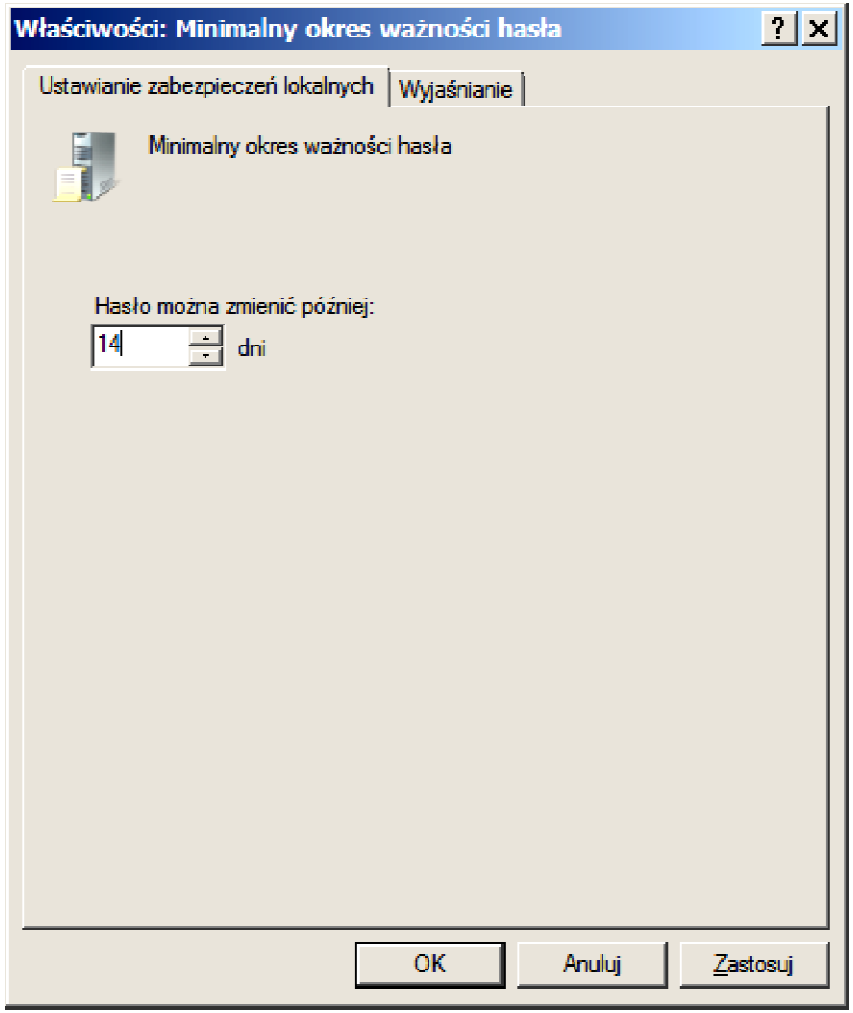
Minimalna długość hasła

- Minimalna długość hasła – określa minimalną liczbę znaków, które musi zawierać hasło



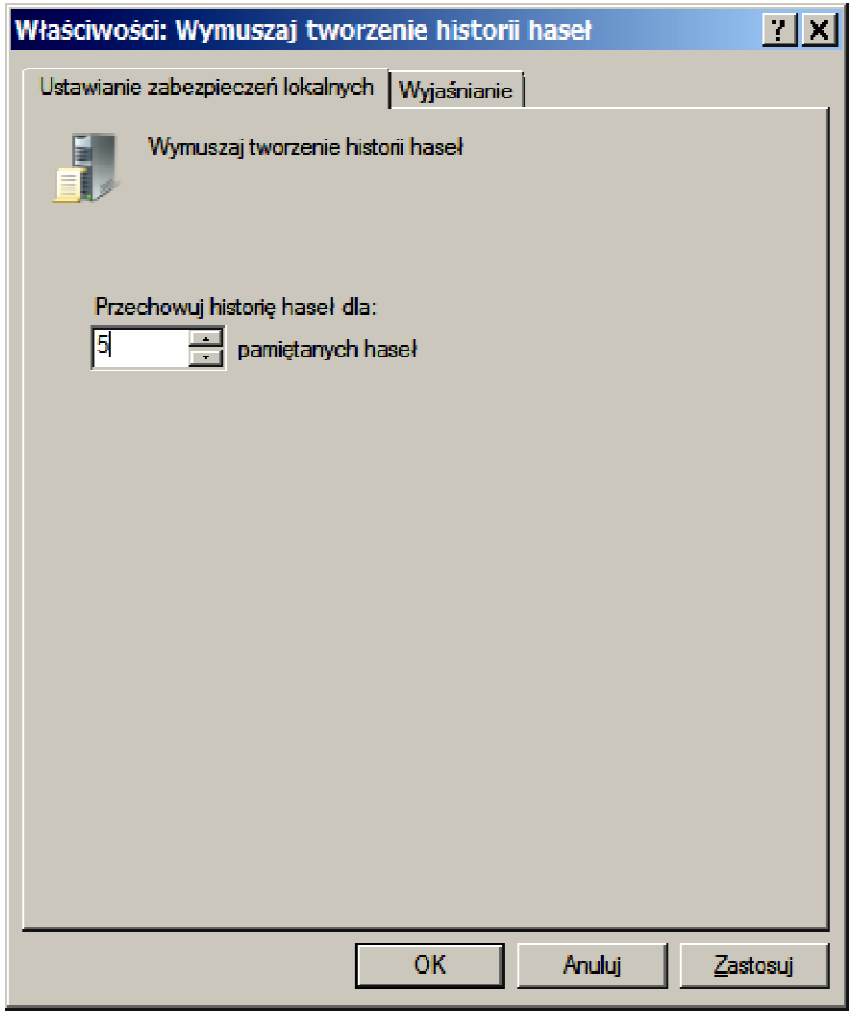
Minimalny okres ważności hasła

- Minimalny okres ważności hasła – ustalamy termin, po którym użytkownik może ponownie zmienić hasło



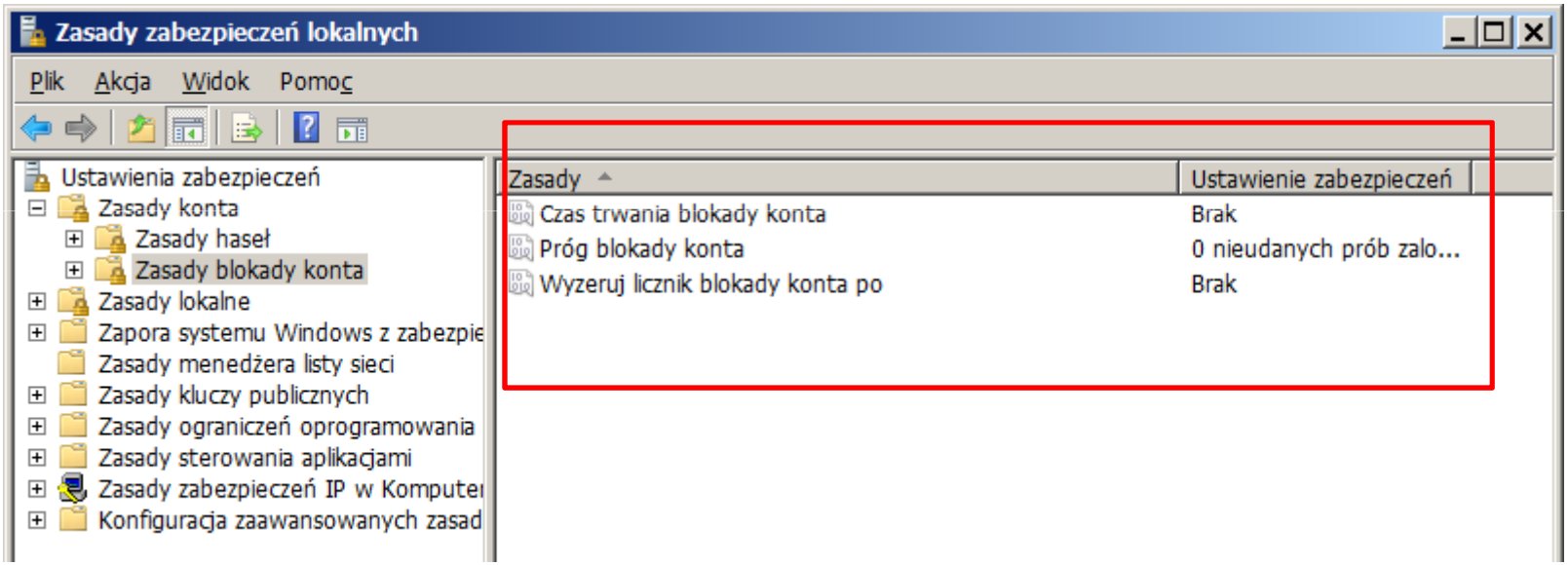
Wymuszaj tworzenie historii haseł

- Wymuszaj tworzenie historii haseł – zasada ta określa, jak często możliwe jest ponowne użycie wcześniej wykorzystywanego hasła, co pozwala zniechęcić użytkowników do praktyk korzystania zamiennie z zestawu standardowych haseł.



Zasady blokady konta

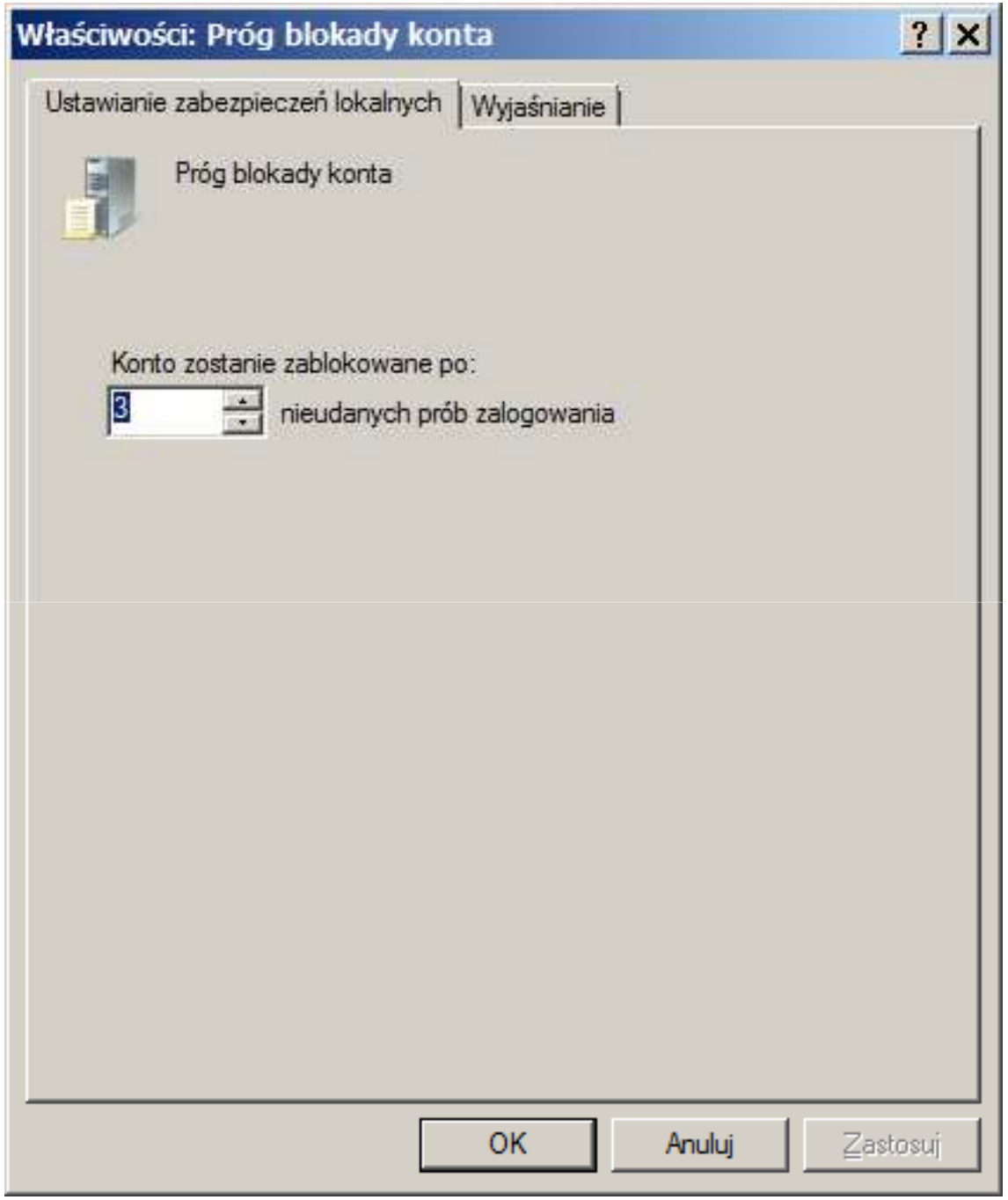
- Poza skonfigurowaniem ustawień dotyczących zasad haseł, należy również ustawić zasady blokowania konta.



- **Czas trwania blokady konta** – To ustawienie zabezpieczeń określa liczbę minut, przez jaką konto pozostaje zablokowane, zanim blokada zostanie automatycznie usunięta. Dostępne są wartości z przedziału od 0 do 99 999 minut. Jeśli czas trwania blokady konta wynosi 0, konto pozostanie zablokowane do momentu, kiedy administrator sam je odblokuje. Jeśli wartość progowa blokady konta jest określona, czas trwania blokady musi być dłuższy lub taki sam, jak czas wyzerowania.


Właściwości: Czas trwania blokady konta
Ustawianie zabezpieczeń lokalnych
Wyjaśnianie
Czas trwania blokady konta
Konto jest zablokowane na:
30
minut
OK
Anuluj
Zastosuj

- **Próg blokady konta** - To ustawienie zabezpieczeń określa liczbę nieudanych prób logowania, która powoduje zablokowanie konta użytkownika. Zablokowanego konta nie można używać do chwili, gdy zostanie ono wyzerowane przez administratora lub gdy upłynie czas blokady. Można ustawić wartość z przedziału od 0 do 999 nieudanych prób logowania. Jeśli zostanie ustawiona wartość 0, konto nigdy nie będzie blokowane. Niepomyślne próby zalogowania do stacji roboczych lub serwerów członkowskich, które zostały zablokowane przez użycie kombinacji klawiszy CTRL+ALT+DELETE lub wygaszaczy chronionych hasłem, nie są traktowane jako nieudane próby logowania.


Właściwości: Próg blokady konta
Ustawianie zabezpieczeń lokalnych
Wyjaśnianie
Próg blokady konta
Konto zostanie zablokowane po:
3
nieudanych prób zalogowania
OK
Anuluj
Zastosuj

- **Wyzeruj licznik blokady konta po** - To ustawienie zabezpieczeń określa liczbę minut, które muszą upłynąć od nieudanej próby logowania, zanim licznik nieudanych prób logowania zostanie wyzerowany i nie będzie wskazywał nieudanych prób logowania. Dostępne są wartości z zakresu od 1 do 99 999 minut. Jeśli jest określona wartość progowa blokady konta, czas wyzerowania musi być krótszy lub taki sam jak Czas trwania blokady konta.


Właściwości: Wyzeruj licznik blokady konta po
Ustawianie zabezpieczeń lokalnych
Wyjaśnianie
Wyzeruj licznik blokady konta po
Wyzeruj licznik blokady konta po
30
minutach
OK
Anuluj
Zastosuj

- gpedit.msc – otwiera konsolę ***„Edytor lokalnych zasad grupy***’