# Polityka haseł w programie BeSTi@ / SJO BeSTi@

## Wstęp

Począwszy od wersji 7.060.00.24 w systemach BeSTi@ oraz SJO BeSTi@ udostępniono funkcjonalność umożliwiającą wdrożenie polityki haseł dla użytkowników ww. systemów.

Po aktualizacji ww. systemów mechanizmy związane z polityką haseł nie będą automatycznie uruchomione lecz będą wymagać samodzielnej konfiguracji zgodnie z wymaganiami polityk bezpieczeństwa każdej instytucji korzystającej z bazy systemu.

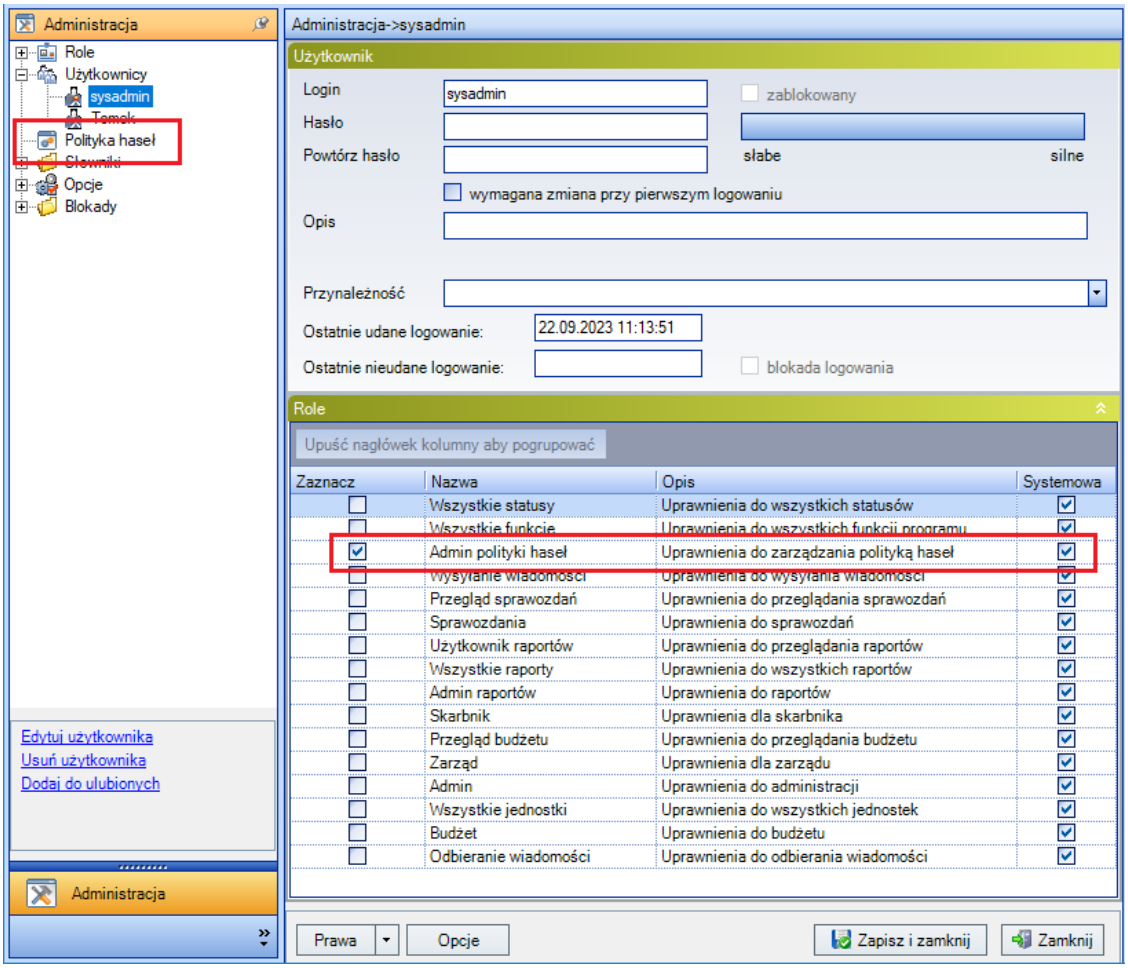
Włączenie polityki haseł wpłynie (w zależności od konfiguracji) m.in. na wymaganą złożoność oraz częstotliwość zmiany hasła, a także pojawią się ewentualne blokady loginów (czasowe lub stałe) użytkowników, którzy podczas logowania kilkukrotnie wprowadzili błędne hasło.

Przed uruchomieniem polityki haseł użytkowników systemu BeSTi@ zaleca się poinformowanie wszystkich użytkowników systemu z danej instytucji o wprowadzeniu nowych wymagań co do częstotliwości oraz złożoności haseł, a także o sposobie postępowania w przypadku zablokowania konta.

Podczas konfiguracji polityki haseł należy wziąć także pod uwagę, że dotyczy ona **wszystkich kont zdefiniowanych w systemie**, w tym także kont posiadających uprawnienia administratora (w tym konta administratora systemowego – sysadmin).

## 1. Ustawienia polityki haseł

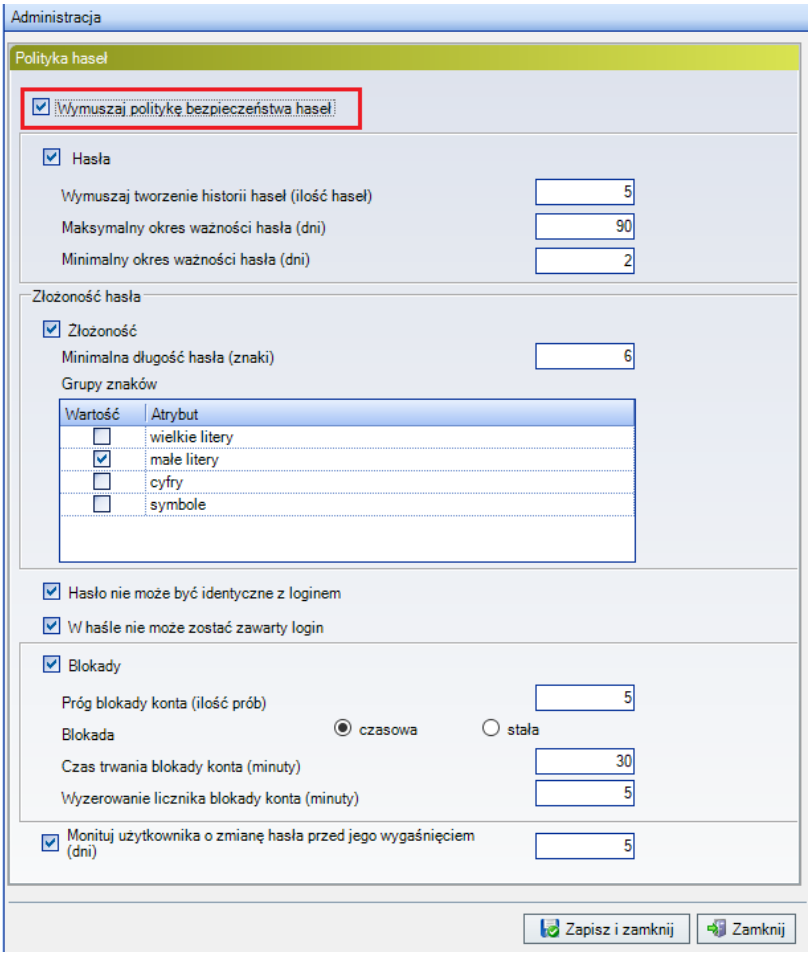
Ustawienia dotyczące polityki haseł dostępne są domyślnie z poziomu konta administratora systemu (sysadmin). Znajdują się w module **Administracja** w gałęzi **Polityka haseł**. Administrator systemu posiada przypisaną automatycznie dedykowaną rolę „Admin polityki haseł".




Uwaga: dostęp do tych ustawień może posiadać również inny uprawniony użytkownik, jeżeli rola ta zostanie mu manualnie przypisana przez administratora. Analogicznie, ustawienia znajdują się z module **Administracja** w gałęzi **Polityka haseł**.

## 2. Poszczególne opcje polityki haseł

Podczas konfigurowania ustawień haseł w pierwszej kolejności należy zdecydować, czy i które opcje będą obowiązywały. By zaznaczyć spersonalizowane ustawienia należy rozpocząć od zaznaczenia *checkboxa* „**Wymuszaj politykę bezpieczeństwa haseł**” wówczas odblokowane do edycji zostaną pozostałe pola. Poszczególne grupy opcji można dowolnie włączać i wyłączać. Warunkiem zapisania ustawień jest zaznaczenia co najmniej jednej grupy.




Minimalne i maksymalne wartości w poszczególnych polach:

**Hasła**

| Opcja | Minimalna możliwa wartość | Maksymalna możliwa wartość | Wartość domyślna |
|---|---|---|---|
| Wymuszaj tworzenie historii haseł (ilość różnych haseł, które użytkownik musi podać, zanim system operacyjny zezwoli na ponowne użycie starego hasła) | 1 | 20 | 5 |
| Maksymalny okres ważności hasła (dni) | 10 | 365 | 90 |
| Minimalny okres ważności hasła (dni) | 0 | 9 | 2 |

**Złożoność hasła**

| Opcja | Minimalna możliwa wartość | Maksymalna możliwa wartość | Wartość domyślna |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Minimalna długość hasła | 6 | 64 | 12 |
| Grupy znaków | 1 | 4 | 3 |

**Blokady**

| Opcja | Minimalna możliwa wartość | Maksymalna możliwa wartość | Wartość domyślna |
|---|---|---|---|
| Próg blokady konta (ilość prób) | 3 | 10 | 5 |
| Czas trwania blokady konta (minuty) | 10 | 60 | 30 |
| Wyzerowanie licznika blokady konta (minuty) (zarejestrowana liczba nieudanych prób logowania (z powodu podania błędnego hasła) resetuje się po udanym logowaniu) | 3 | 15 | 5 |

Uwaga: powyższe wartości obowiązują jedynie w przypadku, gdy zaznaczona jest opcja „**Blokada czasowa**". W przypadku wybrania opcji „**Blokada stała**" możliwość konfiguracji czasu trwania blokady oraz wyzerowania licznika blokady zostaje wyłączona.

**Pozostałe opcje**

- hasło nie może być identyczne z loginem

- w haśle nie może zostać zawarty login

- monituj użytkownika o zmianę hasła – opcja ta określa, z jakim wyprzedzeniem (w dniach) użytkownicy są ostrzegani, że używane przez nich hasło niedługo przestanie obowiązywać.

| Opcja | Minimalna możliwa wartość | Maksymalna możliwa wartość | Wartość domyślna |
|---|---|---|---|
| Monituj użytkownika o zmianę hasła przed jego wygaśnięciem (dni) | 1 | 14 | 5 |

## 3. Informacje dla użytkownika dotyczące stanu logowania i hasła

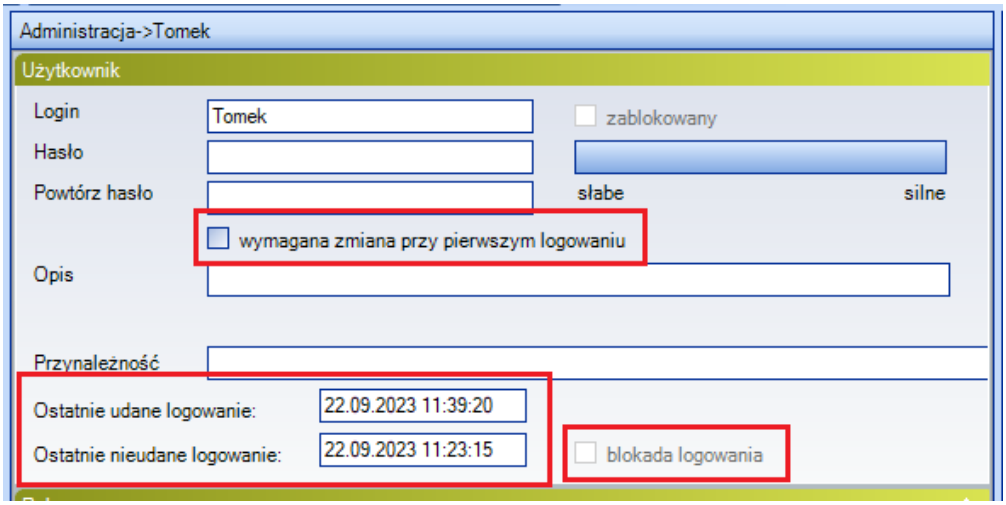
Na górnej belce w programie wyświetlają się następujące informacje:

- ostatnie **udane logowanie** – widoczna jest data i godzina poprzedniego (nie bieżącego) udanego logowania

- ostatnie **nieudane logowanie** (jeśli takie miało miejsce, na przykład w sytuacji pomyłki we wpisywaniu hasła bądź w sytuacji, gdy podczas logowania została wymuszona zmiana hasła)

- **okres ważności hasła** – jeżeli ustanowiony został okres ważności hasła, w tym miejscu program informuje, ile dni pozostało do zmiany hasła.

Informacje o udanym oraz nieudanym logowaniu widoczne są również z poziomu formatki użytkownika w module Administracja na gałęzi Użytkownicy. Znajdują się tam również opcje:




- **wymagana zmiana przy pierwszym logowaniu** – opcja, jeżeli zaznaczona przez administratora podczas tworzenia konta wymusi na nowym użytkowniku zmianę hasła podczas pierwszego logowania do programu

- **blokada logowania** – pokazuje ona status danego użytkownika; jeżeli użytkownik przekroczy próg błędnych logowań (zarówno przy blokadzie czasowej jak i stałej), w tym miejscu pojawi się informacja o jego zablokowaniu.

## Blokada konta

System odnotowuje każde nieudane logowanie danego użytkownika. Jeżeli liczba nieudanych prób logowania przekracza liczbę określoną w opcji, to konto danego użytkownika zostaje zablokowane zgodnie z wybraną opcją (**blokada stała** lub **czasowa**).

- **czasowa blokada logowania** – czasowo blokuje możliwość zalogowania się. Po określonym w opcjach („Czas trwania blokady konta (minuty)”) czasie konto odblokowuje się automatycznie. Blokada może być również zniesiona przez administratora lub użytkownika posiadającego odpowiednie uprawnienia poprzez odznaczenie opcji „blokada logowania” na formatce użytkownika w module Administracja na gałęzi Użytkownicy.

- **stała blokada logowania** – zablokowana zostaje możliwość zalogowania. Zablokowane konto może zostać odblokowane przez administratora systemu lub innego użytkownika posiadającego odpowiednie uprawnienia.

Bez względu na rodzaj blokady, po przekroczeniu liczby prób podczas wpisywania hasła i zablokowaniu możliwości logowania należy zwrócić się do administratora systemu bądź użytkownika posiadającego odpowiednie uprawnienia.