Broszura informacyjna

BEZPIECZEŃSTWO I ZARZĄDZANIE TOŻSAMOŚCIĄ

NetIQ® SecureLogin

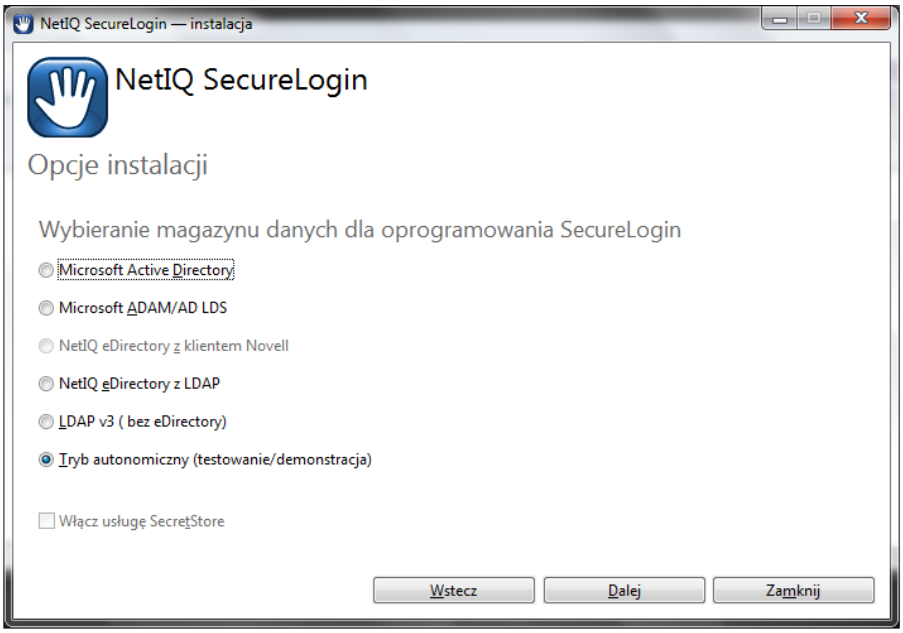
Korporacyjne rozwiązanie do jednokrotnego logowania, zapewniające prosty i kontrolowany dostęp do aplikacji, bezpieczne zarządzanie hasłami oraz uwierzytelnianiem użytkowników do dowolnych aplikacji

System jednokrotnego uwierzytelniania (SSO)

Oprogramowanie SSO (*ang. Single Sign On lub Enterprise Single Sign On*) realizuje funkcję jednokrotnego logowania się użytkowników do dowolnych aplikacji i systemów. Zapewnia bezpieczne i jednokrotne uwierzytelnienie do różnych aplikacji bez konieczności ich zmiany lub modyfikacji. Takim oprogramowaniem jest NetIQ SecureLogin dostępny w polskiej wersji językowej. Obsługuje on między innymi:

- Aplikacje okienkowe pracujące za pomocą grubego klienta w systemie Microsoft Windows XP, Vista, Windows 7 i Windows 8.1, 10 lub serwerach MS Windows,
- Aplikacje pracujące na komputerach Linux i Unix dostępne dla użytkownika przez emulatory terminali pracujące na stacjach Microsoft Windows,
- Środowiska terminalowe Microsoft Terminal Services i Citrix,
- Dostęp do witryn WWW i aplikacji webowych z przeglądarek Microsoft Internet Explorer, Firefox oraz Chrome
- Aplikacje Flash,
- Aplikacje .NET,
- Aplikacje Java,
- Oracle Forms,
- SAP R/3 Login.

NetIQ SecureLogin bazuje na autoryzacji do usług katalogowych i może być wykorzystywany w dowolnym środowisku serwerów i usług katalogowych.



Rys. 1 *W trakcie instalacji NetIQ SecureLogin 8 można wskazać preferowany magazyn danych dla oprogramowania SecureLogin, w tym usługi katalogowe Microsoft Active Directory czy NetIQ eDirectory.*

Oprogramowanie NetIQ współpracuje z usługami katalogowymi Microsoft Active Directory, NetIQ eDirectory i innymi zgodnymi z LDAP v3. W nich w sposób zaszyfrowany przechowuje informacje o kontach użytkowników i ich hasłach do obsługiwanych przez SecureLogin aplikacji i systemów, a także przygotowane wzorce aplikacji

do obsługi SSO. W przypadku usługi katalogowej Microsoftu może być również wykorzystywany tryb Active Directory Application Mode (ADAM) i Lightweight Directory Services (AD LDS).

Przechowywane w systemie katalogowym hasła i informacje uwierzytelniające są zaszyfrowane i objęte dodatkową ochroną – administratorzy mogą jedynie resetować hasła, ale nie mają szans na ich odczytanie lub przejęcie przez zmianę hasła użytkownika do firmowego katalogu. Jeśli hasło zostało zmienione przez jakąkolwiek inną osobę niż użytkownik (nawet przez uprawnionego administratora), to przy pierwszej próbie zalogowania się do firmowego katalogu przy pomocy nowego hasła pojawi się żądanie udzielenia odpowiedzi na pytanie o hasło pomocnicze (*ang. passphrase*), które zostało uprzednio wprowadzone przez użytkownika w celu dodatkowego szyfrowania i zabezpieczenia jego sekretów. Dla hasła pomocniczego istnieje możliwość określenia wymogów co do długości i stopnia skomplikowania oraz zapisania w systemie katalogowym pytania (bądź listy pytań do wyboru) naprowadzającego użytkownika na właściwą, znaną tylko jemu odpowiedź.

Co ważne, SecureLogin zapewnia centralną administrację oprogramowaniem za pomocą konsoli zintegrowanej z Microsoft Management Console (MMC) do zarządzania katalogami Active Directory. Dzięki ścisłej integracji z usługą katalogową Microsoftu do zarządzania systemem SSO wykorzystywane są natywne mechanizmy bezpieczeństwa i system uprawnień wbudowane w Active Directory.

Jak działa SecureLogin

Poniżej opisany jest krok po kroku typowy scenariusz użycia SecureLogin z punktu widzenia użytkownika:

- Użytkownik autoryzuje się do usługi katalogowej za pomocą hasła lub dowolnych innych metod zaawansowanych obsługiwanych w systemie Microsoft Windows, np. karta inteligentna (*smartcard*),
- SecureLogin, w oparciu o uprawnienia dostępu użytkownika do usługi katalogowej, odczytuje informacje uwierzytelniające,
- Użytkownik uruchamia aplikację wymagającą uwierzytelnienia,
- SecureLogin wykrywa pojawienie się obsługiwanego okna dialogowego i korzystając z definicji aplikacji przygotowanej wcześniej przez administratora i rezydującej w usłudze katalogowej, pobiera dane uwierzytelniające do aplikacji i realizuje automatycznie logowanie do aplikacji.
- Użytkownik rozpoczyna pracę z aplikacją bez konieczności podawania dodatkowych informacji uwierzytelniających.
- Jeśli w systemie SecureLogin nie ma jeszcze informacji uwierzytelniających użytkownika do wybranej przez niego aplikacji, może zostać wyświetlone okno z prośbą o podanie niezbędnych informacji uwierzytelniających, które zostaną zachowane w sposób bezpieczny w usłudze katalogowej i wykorzystywane automatycznie przy kolejnych logowaniach.
- SecureLogin może również w sposób automatyczny obsłużyć proces zmiany haseł w obsługiwanych aplikacjach.

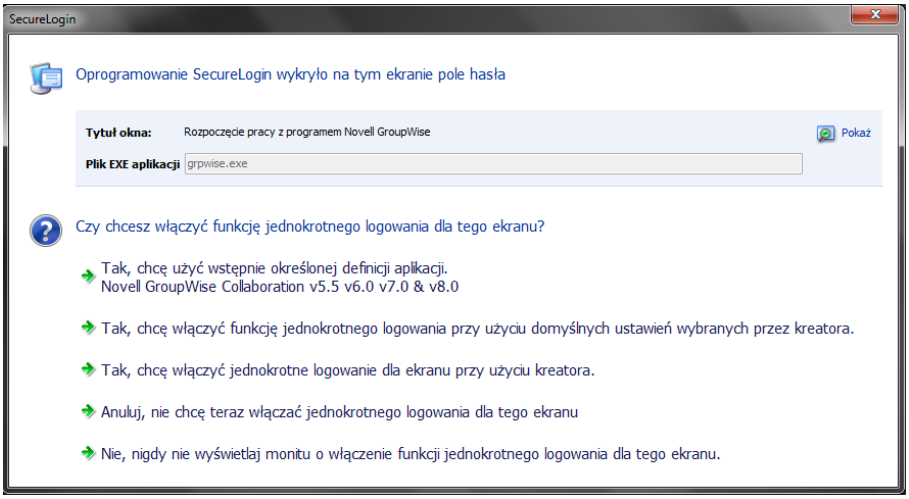
Wygodny interfejs administratora i użytkownika

Oprogramowanie NetIQ SecureLogin jest wyposażone w polską wersję agenta instalowanego na stacjach roboczych użytkowników. Można je łatwo dostosować do specyficznych potrzeb organizacji i np. wyświetlać dodatkowe informacje czy komunikaty dla użytkowników. Do centralnego zarządzania konfiguracją i administracją agentów umieszczonych na stacjach roboczych służy konsola administracyjna dostępna również w jęz. polskim.

Dzięki zastosowaniu oprogramowania agenta nawet zdalni pracownicy, którzy nie mają na stałe połączenia z siecią, mogą korzystać z jednokrotnego logowania, ponieważ NetIQ SecureLogin potrafi lokalnie buforować zaszyfrowane hasła (konfigurowana opcja) .

Administrator systemu SecureLogin ma do dyspozycji graficzne narzędzie obsługiwane również w języku polskim (wizard) służące do przygotowywania wzorców obsługiwanych przez SecureLogin aplikacji i systemów. Z jego pomocą automatycznie przygotuje skrypt do obsługi aplikacji obejmujący kolekcję instrukcji umożliwiających obsługę operacji związanych z rozpoznaniem okienek logowania aplikacji, rozpoznaniem pól do wprowadzania danych w aplikacji, loginem do aplikacji i zmianą hasła w aplikacji.

Dodatkowo SecureLogin został wyposażony w specjalny moduł umożliwiający znalezienie i uzyskanie szczegółowych informacji o aktywnym oknie aplikacji otwartych na stacji Windows. Moduł ten przekazuje precyzyjne informacje z nazwami i identyfikatorami otwartych okienek, co umożliwia weryfikację aplikacji i przygotowanie skryptów do jej obsługi w przypadku, gdy wizard systemu SecureLogin nie wykrył i nie przegotował automatycznie jej obsługi.



Rys. 2. *Przykład działa wizarda oprogramowania SecureLogin tworzącego automatycznie wzorzec obsługiwania aplikacji (w tym przypadku dla systemu poczty Micro Focus Novell GroupWise).*

Wykorzystanie SSO do obsługi komputerów współdzielonych

NetIQ SecureLogin wspiera obsługę SSO na stacjach współdzielonych przez wielu użytkowników (obsługa typu KIOSK).

Automatyzacja obsługi zapomnianego hasła

Wyposażenie pracowników w silne hasło znacznie zwiększa bezpieczeństwo dostępu do cyfrowych zasobów. Nawet w przypadku zapomnienia hasła do usługi katalogowej, proces jego zmiany jest również bezpieczny i – co ważne – zautomatyzowany. Klienci posiadający NetIQ SecureLogin mogą skorzystać z udostępnionego oprogramowania SSPR (*Self Service Password Reset*). Instalując SSPR w formie portalu webowego działającego na platformie Windows lub Linux umożliwią użytkownikom samodzielną realizację zmiany hasła w usłudze katalogowej na wypadek, gdyby zostało zapomniane. Wykorzystywany jest w nim mechanizm Challenge/Response (zdefiniowana seria pytań i odpowiedzi).

Administrator konfiguruje mechanizm Challenge/Response poprzez przygotowanie zestawu pytań, które mogą być kombinacją pytań losowych oraz pytań tzw. wymaganych, dla których użytkownicy zdefiniują odpowiedzi. Podanie poprawnej odpowiedzi jest konieczne do sprawdzania autentyczności użytkownika, gdy użytkownik próbuje zresetować swoje hasło do usługi katalogowej. W systemie SecureLogin administrator może zdefiniować zarówno minimalną liczbę pytań losowych, jak i minimalną liczbę poprawnych odpowiedzi.

Proces zmiany hasła przebiega zgodnie z polityką obsługi haseł. Ta może być definiowana przez administratorów i następnie wymuszana na użytkownikach w trakcie procesu resetu zapomnianego hasła do usługi katalogowej.

Bezpieczeństwo

Oprogramowanie NetIQ SecureLogin szyfruje wszystkie przechowywane nazwy użytkowników i hasła za pomocą klucza AES 256-bitowego oraz mechanizmów zapewnianych przez infrastrukturę PKI. Zostało także wyposażone w mechanizmy zabezpieczające dostęp do danych potrzebnych do logowania użytkownika przez inne osoby, w tym przez administratora systemu czy administratora wykorzystywanych przez SSO usług katalogowych.

SecureLogin można tak skonfigurować, by wymuszał na użytkownikach konieczność podania własnego hasła użytkownika do domeny Microsoft Windows przy logowaniu się do wybranych aplikacji (bez konieczności wprowadzania żadnej zmiany po stronie aplikacji). Po uruchomieniu aplikacji przez użytkownika system SSO poprosi użytkownika o podanie jego hasła do domeny Windows i dopiero po poprawnej autoryzacji loguje użytkownika do aplikacji.

Nawet jeśli uwierzytelnianie do aplikacji ma polegać wyłącznie na podaniu samego hasła, SecureLogin zwiększa bezpieczeństwo tego procesu poprzez kontrolę charakterystyki hasła definiowanego przez użytkownika. Jeśli użytkownik ma do zapamiętania tylko jedno hasło, wówczas może ono mieć trudniejszą do złamania postać, np. odpowiednią długość, czy liczbę znaków numerycznych zawartych w haśle. Inne hasła będą już automatycznie generowane przez NetIQ SecureLogin i mogą mieć bardzo skomplikowaną strukturę, gdyż użytkownik ich nie widzi i nie musi pamiętać.

Dodatkowo przed zalogowaniem użytkownika do aplikacji NetIQ SecureLogin może wymusić ponowne uwierzytelnienie użytkownika oparte o jego hasło w domenie lub jedną z metod zaawansowanego uwierzytelniania. Dzięki temu zabezpieczamy skuteczniej dostęp do dowolnych aplikacji.

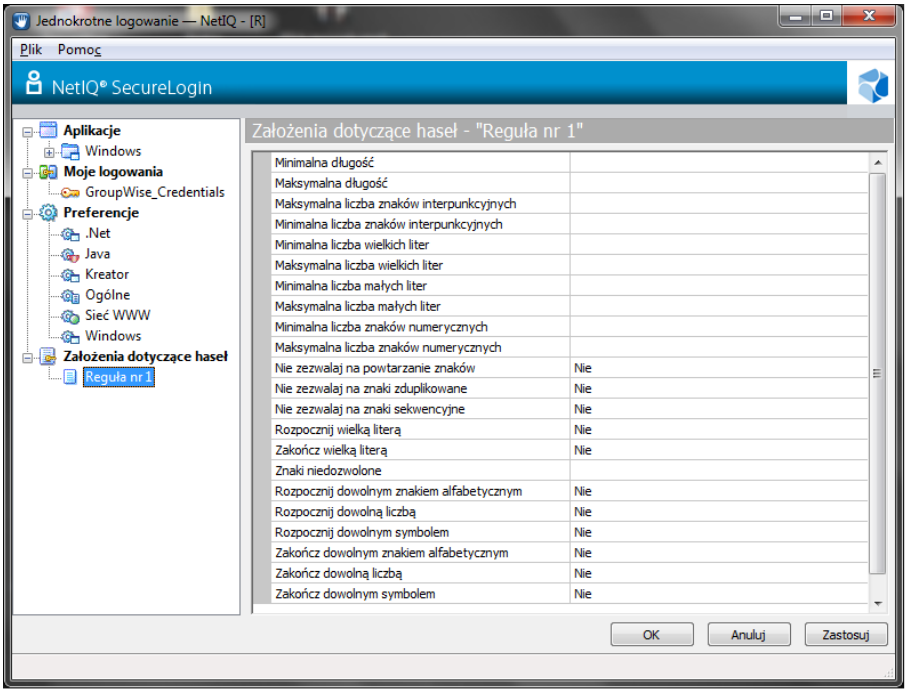
Definiowanie reguł dla haseł dla poszczególnych aplikacji

Jeśli logowanie do jakiejś aplikacji jest już obsługiwane przez NetIQ SecureLogin, można wówczas wprowadzić i wymusić przy jego pomocy reguły dotyczące długości i skomplikowania hasła oraz częstotliwości jego zmiany, nawet jeśli dana aplikacja nie ma wbudowanych takich mechanizmów. Mechanizm ten zmniejsza podatność aplikacji na ataki typu słownikowego przez wprowadzenie trudniejszych do złamania haseł.

Automatyczne generowanie haseł

SecureLogin zapewnia możliwość losowego generowania haseł według zadanych kryteriów – określonej długości i zgodnych ze zdefiniowanymi zasadami konstrukcji hasła. Dokładając do tego możliwość ukrycia przechowywanych w katalogu firmowym haseł przed użytkownikiem możemy uniemożliwić użytkownikom dostęp

do aplikacji bez zalogowania się do firmowego katalogu. Tylko zalogowani użytkownicy będą automatycznie uwierzytelniani do przydzielonych im aplikacji.



Rys. 3. *SecureLogin pozwala na definiowanie reguł dla haseł do poszczególnych systemów i aplikacji.*

Zaawansowane metody uwierzytelniania

Hasła to jednak nie wszystko. SecureLogin ma już wbudowaną obsługę kart inteligentnych (*ang. SmardCard*), a z uwagi na modularną strukturę łatwo go rozbudować o dodatkowe, mechanizmy dostępne w ramach NetIQ Advanced Authentication (kupowane oddzielnie) służące do obsługi wielu zaawansowanych metod uwierzytelniania, wykorzystujących:

- Hasła jednorazowe (One Time Password) i urządzenia mobilne, np. smartfony.
- Urządzenia biometryczne
- Tokeny sprzętowe,
- Dowolne dyski przenośne USB Flash Drive.

W przypadku stosowania kart inteligentnych, SecureLogin obsługuje całą gamę oprogramowania warstwy pośredniczącej, tzw. middleware:

- ActivClient CSP,
- Gemalto CSP,
- AET SafeSign CSP,
- Athena CSP,
- Fujitsu mPollux DigiSign Smart Card middleware.

Pozwala też na wykorzystanie kart do przechowywania zaszyfrowanych haseł dla zdefiniowanych dla SSO systemów i aplikacji.

Obsługa wielu profili logowania w aplikacjach

Użytkownik aplikacji może korzystać podczas logowania z wielu profili określających jego zakres uprawnień (np. użytkownik aplikacji lub administrator aplikacji). W takiej sytuacji SecureLogin w trakcie logowania udostępni użytkownikowi panel z opcjami do wyboru roli/profilu, na jaki użytkownik chce się zalogować.

Odporność na awarie – backup systemu

Ze względu na przechowywanie przez SecureLogin danych uwierzytelniających do obsługiwanych aplikacji w usłudze katalogowej, podlegają one standardowym mechanizmom zabezpieczenia przed awarią i podwyższonej dostępności, jakie zapewnia sama usługa katalogowa. Dzięki replikacji (rozmieszczeniu kilku kopii firmowego katalogu bądź jego fragmentu na różnych serwerach) dane uwierzytelniające będą nadal dostępne z innych serwerów w wypadku awarii któregokolwiek z nich. Przy stosowaniu standardowych procedur sporządzania kopii zapasowych usług katalogowych zapisane w katalogu dane uwierzytelniające do aplikacji również im podlegają – nie ma potrzeby wprowadzania dodatkowych procedur archiwizacji tych danych oraz ponoszenia kosztów dodatkowych narzędzi do backupu.

Audyt

Wszystkie działa wykonywane przez SecureLogin, w szczególności logowanie do aplikacji, są zapisywane w logu. Dzięki temu mamy możliwość audytu procesu logowania i zmiany haseł w obsługiwanych przez SecureLogin aplikacjach, jak również przekazania tych danych do systemów klasy SIEM (*Security Information and Event Management*), takich jak NetIQ Sentinel.

Podsumowanie

NetIQ SecureLogin to narzędzie do bezpiecznego, jednokrotnego uwierzytelnienia do wszystkich zasobów elektronicznych w sieci. Usprawnia proces logowania użytkowników do różnych aplikacji i systemów. SecureLogin rozpoznaje kiedy zachodzi logowanie, przechwytuje informacje uwierzytelniające użytkownika i bezpiecznie składuje je w usłudze katalogowej. Następnie udostępnia te informacje w odpowiednim formacie podczas kolejnych logowań. W ten sposób pojedynczy system SSO może obsługiwać wiele różnych permutacji kont i haseł. SecureLogin pozwala na uproszenie procesu logowania, wyeliminowanie zapisywania haseł przez użytkowników lub stosowania haseł łatwych do zapamiętania i złamania.

Kluczowe zalety oprogramowania firmy NetIQ:

- Jednokrotne logowanie do wielu aplikacji – w tym do złożonych aplikacji internetowych, emulatorów terminali i aplikacji przygotowanych przez firmowych informatyków,
- Nie trzeba wprowadzać żadnych zmian w obsługiwanych aplikacjach,
- Możliwość zastosowania dodatkowych, w tym zaawansowanych metod uwierzytelniania dla dowolnych aplikacji, bez konieczności ich przystosowywania do tego,
- Ograniczenie ryzyka związanego z niewłaściwym przechowywaniem danych uwierzytelniających,
- Łatwe egzekwowanie korporacyjnej polityki haseł i spełnianie wymagań przepisów,
- Zgodność z różnymi rozwiązaniami katalogowymi (eDirectory, MS Active Directory, OpenLDAP itd.),
- Zerowe nakłady na sprzęt do obsługi systemu SecureLogin,

- Mniejsze obciążenie stanowisk pomocy technicznej (nawet o 80%) i kosztów pomocy technicznej (nawet o 40%),
- Część kompletnego rozwiązania firmy NetIQ do zarządzania tożsamością i dostępem do zasobów, na które składają się NetIQ SecureLogin, NetIQ Identity Manager, NetIQ Access Manager oraz NetIQ Sentinel do monitorowania (SIEM).

Więcej informacji na temat jednokrotnego logowania można znaleźć pod adresem

www.netiq.com/products/securelogin

NETIQ W POLSCE:

SUSE Polska Sp. z o.o.

ul. Postępu 21

02-676 Warszawa

tel. 22 537 5010

bezpłatna infolinia 800 22 66 85

infolinia@netiq.com

© 2016 NetIQ, Inc. Wszelkie prawa zastrzeżone. NetIQ i logo NetIQ są zastrzeżonymi znakami towarowymi firmy NetIQ w Stanach Zjednoczonych i innych krajach. * Wszystkie pozostałe znaki towarowe są własnością odpowiednich podmiotów.