Integracja z OpenID Connect oraz SAML 2.0

Zwiększ bezpieczeństwo i zapewnij sprawne logowanie jednokrotne

Integracja z OpenID Connect i SAML 2.0 umożliwia uwierzytelnianie użytkowników Security Center za pośrednictwem platformy zarządzania tożsamością w organizacji, aby uzyskać sprawne i bezpieczne logowanie jednokrotne (z ang. *single sign-on*, SSO).

Zdecentralizowane ryzyko zarządzania dostępem użytkowników

Dzisiejsi pracownicy codziennie używają coraz bardziej zróżnicowanego ekosystemu aplikacji. Pracownicy często ponownie wykorzystują hasła, pozostawiając konta aktywne nawet po odejściu z firmy. Poleganie na natywnym uwierzytelnianiu w celu zarządzania dostępem do systemów korporacyjnych może narazić Twoją organizację na znaczne ryzyko cyber-bezpieczeństwa. Dotyczy to szczególnie systemów bezpieczeństwa, które kontrolują fizyczny dostęp do organizacji i zawierają poufne dane oraz archiwa wideo.

Połącz swój system zabezpieczeń fizycznych i tożsamość korporacyjną

Security Center integruje się bezpośrednio z programową platformą zarządzania tożsamością w organizacji za pomocą protokołów OpenID Connect lub SAML 2.0, oferując kompleksowe rozwiązanie SSO. Grupy użytkowników Security Center są połączone z grupami platformy tożsamości. Użytkownicy logują się do klienta stacjonarnego Security Desk lub przeglądarki internetowej lub aplikacji Genetec Mobile przy użyciu swojego konta firmowego. Ich poświadczenia są sprawdzane przez platformę tożsamości, natomiast ich uprawnieniami zarządza Security Center Directory.

Obsługa

OpenID

Azure Active Directory

Microsoft Active Directory Federation Services

G Suite

Ping Identity

KEYCLOAK

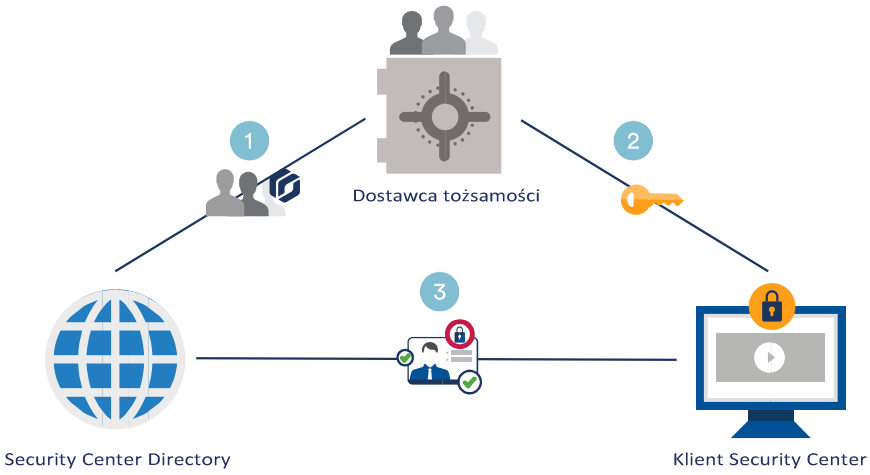
Zastosowanie:
Security Center

Kluczowe korzyści

- Automatycznie aktywuj i aktualizuj konta użytkowników Security Center
- Upewnij się, że nieużywane konta są dezaktywowane, gdy pracownicy opuszczają Twoją organizację
- Zintegruj system bezpieczeństwa fizycznego z platformą zarządzania tożsamością IT
- Skutecznie przestrzegaj strategii SSO Twojej firmy
- Zwiększ komfort użytkowania swoich operatorów bezpieczeństwa

Opis działania

1. Grupy użytkowników Security Center są powiązane z grupami na platformie dostawcy tożsamości.
2. Gdy użytkownik loguje się do aplikacji Security Center, jest on uwierzytelniany za pośrednictwem platformy dostawcy tożsamości. Token jest zwracany dla prawidłowych użytkowników.
3. Uwierzytelnieni użytkownicy dziedziczą swoje uprawnienia z Security Center Directory.

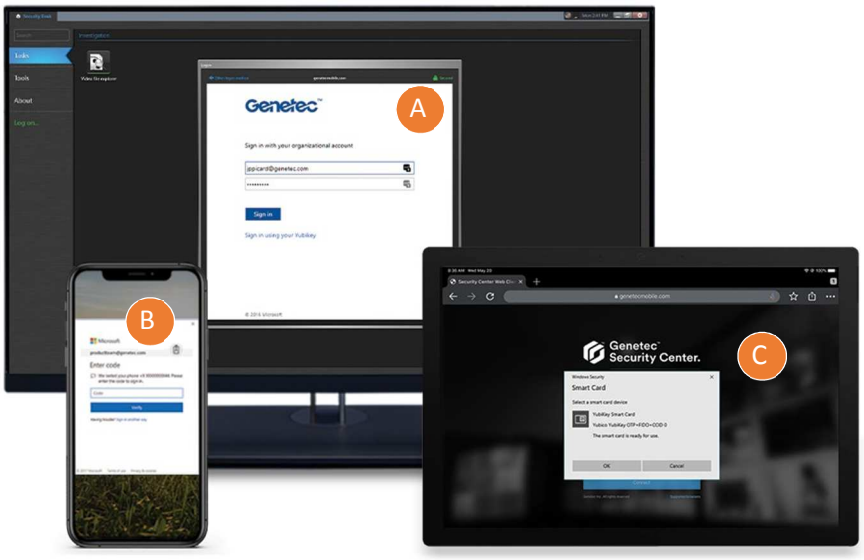


Interfejs użytkownika

A. Osiągnij bezproblemową obsługę dzięki wbudowanym kontom użytkowników zarządzanym przez firmę.

B. Zwiększ bezpieczeństwo, korzystając z możliwości uwierzytelniania wieloskładnikowego dostawcy tożsamości.

C. Obsługiwany przez wszystkich klientów Security Center.



60-545 Poznań, ul. Kajki 1, tel. 61 846 21 00, info@arpol.pl
30-056 Kraków, ul. Bydgoska 6, tel. 12 638 09 73, krakow@arpol.pl
01-410 Warszawa, ul. Czorsztyńska 10A, tel. 22 532 29 80, warszawa@arpol.pl