AuthControl Sentry®

Ochrona tożsamości poprzez inteligentne uwierzytelnianie

Nagradzana technologia AuthControl Sentry® oferuje inteligentne, wieloskładnikowe rozwiązanie uwierzytelniające dla biznesu z technologią stanowiącą podstawę bezpieczeństwa i uwierzytelniania opartego na ryzyku, zapewniającym dynamiczną kontrolę.

swivelsecure

www.swivelsecure.com

Biuro w Wielkiej Brytanii i Irlandii
Północ
1200 Century Way
Thorpe Park
Leeds
LS15 8ZA

Centrala: +44 (0)1134 860 123
Wsparcie techniczne : +44 (0)1134 860 111
hq@swivelsecure.com

Południe
Pinewood
Chineham Business Park
Chineham, Basingstoke
RG24 8AL

Biuro w USA i APAC
Seattle
Swivel Secure, Inc.
1001 4th Ave #3200
Seattle, WA 98154

+1 949 480 3626 (Czas pacyficzny)
Bezpłatna infolinia: 866.963 AUTH (2884)
usa@swivelsecure.com

Biura EMEA
Portugalia
Estrada de Alfragide,
N.º 67, Alfrapark – Lote H,
Piso 0, 2614-519 Amadora

+351 215 851 487
portugal@swivelsecure.com

Hiszpania
Calle Punto Mobi 4,
28805 Alcala de Henares
Madrid

+34 911 571 103
espana@swivelsecure.com

AuthControl Sentry® Inteligentne uwierzytelnianie wieloskładnikowe

Dostępny w ponad 52 krajach i wdrożony w wielu przedsiębiorstwach (finanse, instytucje rządowe, opieka zdrowotna, edukacja i przemysł) AuthControl Sentry® zapewnia prawdziwe uwierzytelnianie wieloskładnikowe, co pozwala w inteligentny sposób zapobiec nieupoważnionemu dostępowi do aplikacji i danych.

Zeskanuj kod QR, aby zobaczyć pełny schemat kompletnego rozwiązania uwierzytelniania wieloczynnikowego AuthControl Sentry®

AuthControl Sentry® posiada dużą elastyczność do obsługi szerokich wymagań systemowych oraz zapewnia maksymalne zaspokojenie potrzeb użytkownika, dzięki swojemu szerokiemu wachlarzowi możliwości autentykacji. Niezależnie od tego czy korzystasz z aplikacji mobilnej, czy najnowszych rozwiązań biometrycznych za pomocą czytnika Fingerprint, AuthControl Sentry® staje się wiodącym rozwiązaniem w dziedzinie cyberbezpieczeństwa.

Co nas wyróżnia?

- Opatentowana technologia PINsafe® zapewniająca najwyższą jakość bezpieczeństwa - patrz strona 8
- Wsparcie u klienta oraz w chmurze dla każdej architektury
- Rozwiązania chmurowe typu single tenancy i single tiered zapewniają optymalną adaptację rozwiązań i kontrolę na każdym etapie wdrożenia
- Uwierzytelnianie risk-based i single sign-on jako standard
- Bezproblemowa integracja z setkami aplikacji
- Zapewnia maksymalną adaptację dzięki szerokiemu wyborowi metod uwierzytelniania – nawet do dziesięciu czynników!

Uwierzytelnij dostęp dla wszystkich, bez względu czy to logowanie do Office 365, transakcja eCommerce czy planowanie zasobów przedsiębiorstwa w systemie ERP.

- ✓ Pracownicy
- ✓ Klienci
- ✓ Dostawcy

Architektura

Wsparcie u klienta oraz w chmurze dla zmiennej architektury

AuthControl Sentry® nie ma żadnych ograniczeń. Jest zaprojektowany do uwierzytelniania dostępu

do zasobów niezależnie od tego, czy są one hostowane w chmurze czy terenie firmy, oraz czy użytkownik jest klientem, pracownikiem czy zewnętrznym dostawcą.

Architektura u klienta

Uzyskaj dostęp do wewnętrznych systemów za pośrednictwem usługi Agent Active Directory. To instalowana lokalnie aplikacja, która eliminuje potrzebę udostępniania usługi Active Directory przez Internet, jednocześnie zachowując synchronizację konta użytkownika.

Architektura oparta na chmurze

Stały adres IP: Każdy klient AuthControl otrzymuje dedykowany stały adres IP dla własnej wirtualnej instancji. Brak współdzielonego zasobu, współużytkowanego interfejsu programowania aplikacji ani współdzielonego portalu wejściowego oraz współużytkowanej bazy danych.

Dedykowana oferta: AuthControl Cloud® zapewnia dedykowaną maszynę wirtualną. Nie ma współdzielonych opcji (multi-tenant), więc możesz oczekiwać całkowitego zarządzania i kontroli, co oznacza, że możesz skonfigurować rozwiązanie w zależności od twoich potrzeb.

Prywatna zapora: Oferujemy dedykowane i niezależne zapory dla każdego klienta, pozwalające dostosować listy bezpieczeństwa i kontroli dostępu.

Cechy

Single Sign-On jako standard

Funkcjonalność SSO dla AuthControl Sentry® to właściwość zapewniająca dostęp do wszystkich aplikacji dzięki jednemu procesowi uwierzytelniania, zapewniając użytkownikom wydajną pracę bez narażania bezpieczeństwa.

Ciągłe bezpieczeństwo

Swivel Secure dostarcza Unified Portal, aby zapewnić użytkownikom wygodny dostęp. Używając jednego miejsca, możesz zarządzać uprawnieniami użytkowników i śledzić ich zachowanie w celach kontrolnych.

Opłacalność

Dzięki wykorzystaniu SSO można osiągnąć duże oszczędności, ponieważ znika potrzeba kontaktu z IT w celu uzyskania hasła. Wydajność wzrasta, gdy użytkownicy logują się tylko raz i uzyskują dostęp do wszystkich swoich aplikacji - oszczędzają czas.

Intuicyjność

SSO ma na celu zwiększenie wydajności poprzez umożliwienie użytkownikom dostępu do wszystkich aplikacji za pomocą mechanizmu opartego na Risk-based policy. Niezależnie od tego, czy użytkownicy uzyskują dostęp do aplikacji przez VPN, “On-premise” lub w chmurze, będą automatycznie skierowani do uwierzytelniania za pomocą funkcji SSO w Unified Portal.

Wdrażaj AuthControl Sentry® dla autentykacji:

- Interesariusze - pracownicy, dostawcy, i klienci
- Dostęp do aplikacji takich jak Office 365, Salesforce lub SAP
- Specyficzny rynek pionowy, taki jak usługi finansowe

Cechy

Autentykacja risk-based jako standard

Risk-based autentication (RBA) jest dynamiczną funkcją AuthControl Sentry ®, zaprojektowany w celu automatycznego żądania odpowiedniego poziomu uwierzytelnienia w celu uzyskania dostępu do aplikacji. W oparciu o parametry ustawione w silniku strategii, RBA zażąda odpowiedniego poziomu uwierzytelnienia, aby uzyskać dostęp do aplikacji na podstawie użytkownika, ich urządzenia i aplikacji.

Dynamiczny i inteligentny

Dostosowuje się do potrzeb użytkownika włącznie z:

- Do jakiej aplikacji próbują uzyskać dostęp
- Do jakiej grupy należy użytkownik
- Skąd uzyskuje dostęp do aplikacji
- Z jakiego urządzenia korzystają

Algorytm polityk

W oparciu o system punktów silnik adaptacyjnej polityki uwierzytelniania umożliwia administratorom ustawianie parametrów dla użytkownika i dla aplikacji

- Członkostwo w grupie
- Dostęp do aplikacji
- Adres IP
- Ostatnie uwierzytelnienie
- Certyfikat X.509
- Urządzenie
- Lokalizacja fizyczna (GeoIP)
- Prędkość zmian geolikalizacji

Autentykacja risk-based: Przykład 1

Asystent zakupów poleciał do Azji Południowo-Wschodniej, aby odwiedzić dostawcę z Menadżerem Zakupów. Właśnie skończyła posiłek w restauracji i zdaje sobie sprawę, że zapomniała sprawdzić zapasy niektórych składników na spotkanie następnego dnia. Pomyślała, że szybko zaloguje się do systemu ERP, korzystając z firmowego urządzenia mobilnego.

System ERP	
Wymaga 120 punktów	
LAN	0
Znany adres IP	0
Zarządzane urządzenie	50
Zakres IP (Azja)	-100
Wymagane uwierzytelnienie	
U&P	10
Mobile App	60
Fingerprint	20

Wynik - nieudany
Chociaż próbuje użyć firmowego telefonu, aby uzyskać dostęp do systemu ERP, zakres IP ustawia minus 100 punktów ze względu na lokalizację. Tym razem nie uzyska dostępu do ERP, niezależnie od tego, czy chce używać uwierzytelniania wieloskładnikowego.

Autentykacja risk-based: Przykład 2

Menedżer sprzedaży pracuje dziś w biurze i chce uzyskać dostęp do CRM, aby zorganizować spotkanie. Używa służbowego laptopa i uzyskuje dostęp do aplikacji znajdującej się w wewnętrznej infrastrukturze firmy.

CRM system	
Wymaga 120 punktów	
LAN	50
Znany adres IP	50
Zarządzane urządzenie	50
Zakres IP (Polska)	50
Wymagane uwierzytelnienie	
U&P	10
Mobile App	60
Fingerprint	20

Wynik - udany
Menedżer sprzedaży wyraźnie przekracza liczbę punktów potrzebnych do uzyskania dostępu do CRM. Po uwierzytelnieniu może użyć funkcji pojedynczego logowania (SSO), aby uzyskać dostęp do innych aplikacji. Otrzymuje połączenie z Asystentem Zakupów i ma dostęp do systemu ERP.

Maksymalna elastyczność i kontrola

Mechanizm zasad pozwala tworzyć nowe reguły i łączyć istniejące reguły, a także zapewnia mechanizm obsługi szeregu scenariuszy o coraz większej złożoności.

Cechy

Portal użytkownika

Portal użytkowników to funkcja programu AuthControl Sentry®, zaprojektowana w celu zapewnienia administratorom konfigurowalnego rozwiązania zapewniającego użytkownikom autonomię w zakresie podstawowych zadań związanych z samodzielną administracją.

Portal użytkownika udostępnia administratorom następujące funkcje - możliwość zapewnienia użytkownikom bezpośredniego dostępu do danych, co pozwala im realizować proste czynności administracyjne takie jak zmiana lub zresetowanie kodu PIN.

Udostępnianie aplikacji mobilnej

Do użytkownika wysyłany jest e-mail ze szczegółami udostępniania aplikacji mobilnej oraz QR kod do konfiguracji. Po konfiguracji użytkownicy mogą uwierzytelniać dostęp do wszystkich swoich aplikacji za pomocą: - kodu jednorazowego (OTC) lub - powiadomienia PUSH.

Samoobsługa

Samoobsługowy portal użytkownika zmniejsza koszty które zwykle związane są ze wsparciem.

Większa wydajność

Swivel Secure User Portal został tak zaprojektowany, aby zapewnić użytkownikom większą wydajność w wykonywaniu podstawowych zadań, w tym:

- Zmiana kodu PIN
- Resetowanie kodu PIN
- Udostępnianie aplikacji mobilnej
- Ponowna synchronizacja tokena sprzętowego.

Można wprowadzić ograniczenia w celu upewnienia się, że metody i sposoby autentykacji są zgodne z protokołami bezpieczeństwa.

Technologia

swivelsecure

Opatentowana technologia PINsafe®

PINsafe® to opatentowana technologia, która obsługuje składniki uwierzytelniania takie jak PINpad®, PICpad i TURING. Należy do szeregu czynników uwierzytelniania dostępnych w AuthControl Sentry® - rozwiązania do uwierzytelniania wieloskładnikowego zaprojektowanego w celu ochrony organizacji przed nieautoryzowanym dostępem do ich aplikacji, sieci i danych.

Jak działa PINsafe®?

Każdy użytkownik otrzymuje PIN - jednak ten kod PIN nigdy nie jest wprowadzany.

Gdy użytkownik musi bezpiecznie się uwierzytelnić, zostanie mu udostępniony 10-znakowy łańcuch bezpieczeństwa – sekwencja znaków lub cyfr. Ciąg bezpieczeństwa może być wyświetlany jako grafika (TURing, PINpad® or PICpad) lub można go wysłać pocztą e-mail lub za pomocą weryfikacji SMS.

Używając kodu PIN jako wskaźnika położenia, można wyodrębnić jednorazowy kod uwierzytelniający.

Przykład poniżej

Przykład pokazuje, że kod PIN to 1370. W tym przypadku ciąg zabezpieczeń to 5721694380, więc kod logowania to 5240

Ciąg bezpieczeństwa można zintegrować z wieloma urządzeniami i aplikacjami na różne sposoby, aby uzyskać pełną elastyczność. Przykłady wykorzystania:

- Logowanie do systemu Windows
- Zdalny dostęp do F5, Citrix Netscaler i Cisco VPN
- Dostęp do sieci za pomocą OWA, Apache i Microsoft ILS

Your PIN	1		3			7		0	
Encrypted Security No.	5	7	2	1	6	9	4	3	8	0
Your one time code	5		2			4		0	

PINsafe® uniemożliwia użytkownikowi wprowadzenie kodu PIN, zapobiega infiltracji, takiej jak ataki typu „man-in-the-middle”.

Składniki

Składniki uwierzytelnienia

Swivel Secure zapewnia szeroką gamę składników uwierzytelniania, aby zapewnić maksymalne dopasowanie w całej organizacji

Niezależnie od tego, czy zdecydujesz się na uwierzytelnianie za pomocą OTC w aplikacji mobilnej (AuthControl Mobile®, tradycyjny token sprzętowy, czy nawet za pomocą odcisku palca), AuthControl Sentry® Swivel Secure zapewnia najwyższe bezpieczeństwo i możliwość konfiguracji w celu dostosowania do potrzeb Twojej organizacji.

AuthControl Mobile®: OTC

Za każdym razem, gdy zostaniesz poproszony o uwierzytelnienie, po prostu skorzystaj z OTC wyświetlanego w aplikacji. Ponieważ jest 99 kodów, funkcja OTC jest na tyle wszechstronna, że można jej używać w trybie offline. Po wprowadzeniu kodu uzyskasz dostęp do swojej aplikacji.

Czynnik obrazkowy: PINpad®

10-cyfrowy kod jest przedstawiany w postaci siatki liczb w przeglądarce internetowej użytkownika. Użytkownik po prostu klika na obrazy które reprezentują ich PIN. Następnie po kliknięciu zostanie przesłany inny kod TC do Auth Control Sentry® dla uwierzytelnienia użytkownika.

Czynnik obrazkowy: PICpad

PICpad to czynnik uwierzytelniający, który omija bariery językowe.

Korzystając z tych samych zasad, co PINpad®, PICpad wyświetla symbole zamiast cyfr, zapewniając spójne znaczenie w środowiskach wielonarodowych.

AuthControl Mobile®: PUSH

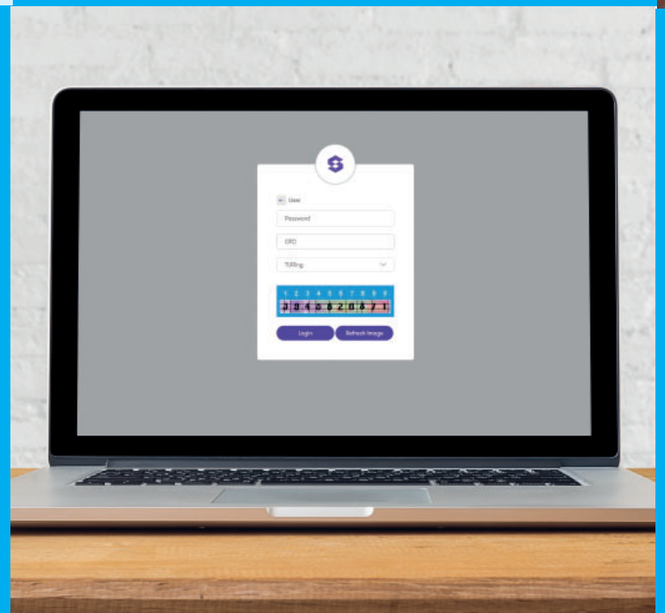
Powiadomienie wysyłamy bezpośrednio na Twój telefon komórkowy. Wystarczy nacisnąć przycisk w aplikacji mobilnej, aby potwierdzić uwierzytelnienie.

Funkcja Swivel One Touch® jest prosta we wdrożeniu i wymaga minimalnej konfiguracji.

Czynnik obrazkowy: TURing

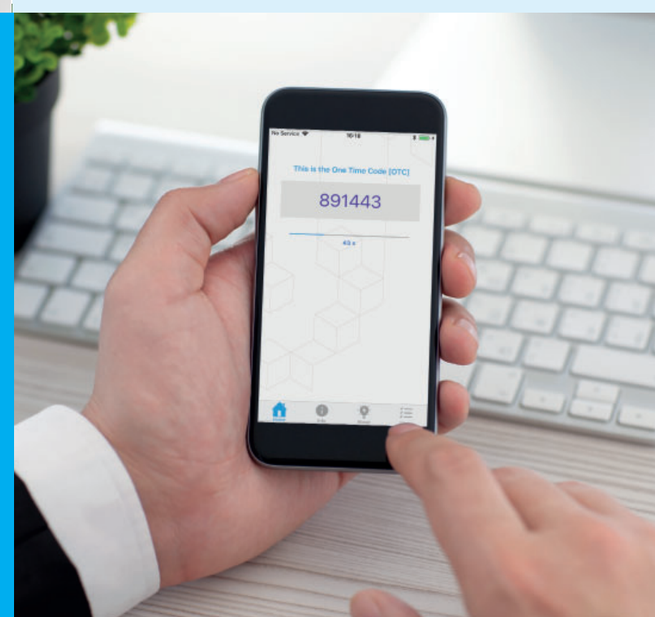
10-cyfrowy kod jest prezentowany w formularzu prostokątnego obrazu w przeglądarce internetowej użytkownika. Użytkownik wybiera numery wskazane przez swój PIN.

Przykład: Jeśli ich kod PIN to 1370, to następnie wybierają znaki 1, 3, 7 i 10 z prezentowanego obrazu.



AuthControl Mobile®: OATH

OATH soft token - jest tokenem opartym na czasie, licząc od 0 do 60, podobny do tradycyjnego tokena sprzętowego używanego do uzyskiwania dostępu do aplikacji przez VPN. OATH zapewnia użytkownikowi sześciocyfrowy kod uwierzytelniający.



Mobile: SMS

Aby chronić OTC (wysyłanym przez SMS) przed przechwyceniem, treść SMSa jest chroniona przez mechanizm PINsafe®. Oznacza to, że SMS zawiera ciąg bezpieczeństwa o wartości dwóch sekwencji alfanumerycznych, co w połączeniu z kodem PIN użytkownika, tworzą jego OTC.

Biometria: odcisk palca

Rozpoznawanie odcisków palców jest dostępne dla AuthControl Credential® Provider przy użyciu struktury biometrycznej Windows 10 i kontrolera dostępu odcisków palców NITGEN. Użytkownicy mogą uwierzytelniać się za pomocą kontrolera linii papilarnych NITGEN lub wbudowanego czytnika linii papilarnych w swoim laptopie.

AuthControl Voice

Dzwoniąc do użytkownika, AuthControl Voice wokalizuje albo kod jednorazowy (OTC), albo powiadomienie PUSH (TAK lub NIE) w celu uwierzytelnienia dostępu do aplikacji. OTC dostarczane głosowo przez telefon jest następnie wpisywane w oknie na żądanie.

Token sprzętowy

Token sprzętowy zapewnia użytkownikom jednorazowy kod (OTC), dzięki czemu mogą bezpiecznie się logować do swoich aplikacji. Za każdym razem, gdy przycisk jest wciśnięty, pojawia się nowy kod, co gwarantuje, że dostęp osób nieupoważnionych nie jest możliwy.

swivelsecure

Integracje

AuthControl Sentry® to jedno z najbardziej elastycznych rozwiązań na rynku, integrujące się z setkami aplikacji i urządzeń, za pośrednictwem RADIUS, ADFS, SAML i naszego własnego zastrzeżonego API - AgentXML.

Niezależnie od tego, czy potrzebujesz dostępu do Salesforce, uwierzytelniania za pomocą aplikacji mobilnej, czy logowania do dostawcy poświadczeń systemu Windows za pomocą obrazu uwierzytelniającego, AuthControl Sentry® obsługuje szeroką gamę aplikacji i urządzeń, zapewniając elastyczność i wydajność wymaganą do bezproblemowego uwierzytelnienia w całej organizacji.

Licencjonowanie

Modele cenowe odpowiednie dla wszystkich organizacji. Licencjonowanie jest określane na podstawie pojedynczego użytkownika systemu.

Licencjonowanie użytkownika

Elastyczne plany licencjonowania i modele cenowe odpowiednie dla wszystkich organizacji.

- Jedna licencja AuthControl Sentry® dotyczy jednego użytkownika
- Każda licencja zawiera WSZYSTKIE czynniki uwierzytelnienia
- MFA, SSO i RBA są zawarte w AuthControl Sentry®
- Dostępne jako kontrakty na 1, 3, 5 lub 7 lat oraz na warunkach wieczystych.

On-Premise

Wieczysta licencja jest dostępna dla rozwiązania On-premise lub w prywatnej chmurze. Cena jest ustalana w przeliczeniu na użytkownika, na skali przesuwnej, zaczynając od 10 użytkowników. Ceny są kumulatywne, więc jest to wyjątkowo opłacalny sposób na zakup licencji. Idealnie nadaje się dla organizacji, które chcą z góry zaoszczędzić na kosztach usługi wraz ze stabilną ilością użytkowników.

Chmura

Licencje na jeden rok (Subscription licensing) są dostępne w chmurze. Pozwala to również organizacjom spełnić wymagania użytkowników wg zmian popytu. Brak kosztów wstępnych, a umowa jest elastyczna i wolna od kar.

Opcje licencjonowania

Skorzystaj z poniższej tabeli, aby porównać opcje licencjonowania On-premise i chmurowego

Rodzaj licencji	On-Premise	Chmura
Risk-based Authentication	✓	✓
Integracje (SAML/ADFS/RADIUS)	✓	✓
Aplikacje On-premise i w chmurze	✓	✓
Wszystkie czynniki uwierzytelnienia	✓	✓
AD Agent & AD Sync	✓	✓
Unified Portal w połączeniu z Single sign-on	✓	✓
Raportowanie	✓	✓
Sprzęt (Physical/Virtual)	✓	✗
Obraz Amazon AWS	✗	✓
24x7x365	Opcjonalne	✓

Serwis i wsparcie

Aby zapewnić organizacjom dostęp do pomocy technicznej oraz aktualizacji, oferujemy poziom wsparcia Standard i Premium dla naszej platformy uwierzytelniania. Dostępne również profesjonalne usługi przeprowadzania aktualizacji, wdrażania, migracji i kompleksowej integracji.

Podstawowa umowa serwisowa

Godziny wsparcia: 8/5. Dostęp do aktualizacji oprogramowania i poprawek błędów.

Standardowa umowa serwisowa

Godziny wsparcia: 24/5. Swivel Secure oferuje standardowe wsparcie 24 godziny na dobę w dni robocze.

Umowa serwisowa Premium

Godziny wsparcia: usługa 24/7, idealny dla dużych firm wymagających natychmiastowej pomocy ekspertów.

Profesjonalne usługi

Swivel Secure zapewnia szereg profesjonalnych usług dla organizacji, wymagających dodatkowych lub dostosowanych zasobów technicznych podczas wdrażania uwierzytelniania wieloskładnikowego i zapewniania zgodności z systemami, połączeniami i sprzętem.

Usługa Technical Account Manager (TAM)

Nasza usługa TAM zapewnia proaktywne wskazówki i scentralizowane zarządzanie usługami, zapewniając korzyści z priorytetowej obsługi w ramach każdego kanału wsparcia.

Chcesz zaktualizować urządzenie Swivel Secure?

Swivel Secure rozpoznaje niektóre problemy, które mogą wystąpić podczas aktualizacji i oferuje usługę aktualizacji opracowaną tak, aby zapewnić minimalne zakłócenia działania.

Czy masz bardzo złożoną infrastrukturę sieciową, która wymaga wielu integracji?

Nasz zespół ekspertów może ściśle współpracować z inżynierami technicznymi Twojej firmy, aby zapewnić:

- Każdy proponowany projekt jest dostosowany do architektury sieciieci
- Projekt spełnia architektoniczne wymagania organizacji oraz kontrolę zmian

Potrzebujesz zintegrować nowe urządzenie RADIUS lub SAML bez wcześniejszej integracji?

Nasz zespół programistów może być pod ręką:

- Aby ocenić i opracować nowe integracje
- Aby zintegrować nowe wtyczki
- Aby spełnić oczekiwania dotyczące zmian w oprogramowaniu.