

WEBCON

AI Proxy Self-hosted

1.0.0.235

historia zmian wersji 1.0.0.235

1. Nowości

- Opublikowano **AI Proxy Self-hosted** – nowy komponent, który umożliwia klientom korzystanie z funkcjonalności AI w WEBCON w oparciu o własną infrastrukturę, z całkowitym pominięciem infrastruktury WEBCON. Rozwiązanie jest dostępne w licencji subskrypcyjnej Enterprise oraz w licencji wieczystej WEBCON Agentic AI Framework.

Udostępniono możliwość instalacji AI Proxy Self-hosted w środowisku klienta (on-premise lub prywatna chmura) wraz z opcją podpięcia i konfiguracji własnych modeli AI – hostowanych w Google Vertex, OpenAI lub Azure AI Foundry. Dzięki temu klienci zyskują pełną kontrolę nad danymi i infrastrukturą wykorzystywaną do przetwarzania AI, co ułatwia spełnienie wymogów bezpieczeństwa, polityk prywatności oraz regulacji branżowych.

Wprowadzono dedykowany tryb AI Proxy Self-hosted oraz nowy węzeł konfiguracyjny, dodany w plikach konfiguracyjnych `appsettings.json` wykorzystywanych do uruchamiania AI Proxy, dla tego trybu, obejmujący:

- możliwość włączenia użycia AzureKeyVault do przechowywania danych wrażliwych,
- zmienną przechowującą ścieżkę dostępu do certyfikatu `.pem` lub `.pfx` oraz hasło.

Przygotowano także alternatywną implementację klas, która w tym trybie umożliwia zastąpienie Azure Key Vault zmiennymi środowiskowymi.

Zaprojektowano i udostępniono nowy, ujednoczony model konfiguracji dostawców AI oparty o priorytety. Umożliwia on definiowanie wielu dostawców, automatyczne przełączanie na dostawców o niższym priorytecie oraz przypisywanie różnych modeli AI do poszczególnych metod (modele tekstowe, obrazowe i audio). Konfiguracja jest wykonywana w pliku `aiconfiguration.json`, który jest wczytywany podczas uruchamiania aplikacji AI Proxy.

Dodano możliwość wyboru trybu działania aplikacji w pliku konfiguracyjnym oraz obsługę lokalnych certyfikatów (`.pem/.pfx`) wykorzystywanych do podpisywania i weryfikacji tokenów dostępowych – bez konieczności komunikacji z zewnętrznymi usługami autoryzacyjnymi (w tym z LAS) czy bazami danych. W trybie AI Proxy Self-hosted ograniczono zależność od zewnętrznych komponentów infrastrukturalnych: aplikacja może działać bez połączeń do usług licencyjnych, baz danych oraz magazynów danych w chmurze, a wymagane mechanizmy są dobierane automatycznie na podstawie konfiguracji.