

Interfejs API baramundi Proactive Connect

*Ukierunkowana integracja danych z punktów
końcowych – interoperacyjność jako podstawa
nowoczesnych infrastruktur IT*

Streszczenie

Środowiska IT rozwijają się dzięki wymianie danych – bez ręcznej interwencji – między różnymi narzędziami. baramundi Proactive Hub gromadzi i analizuje wskaźniki wydajności i stabilności, a także wskaźniki bezpieczeństwa, umożliwiając proaktywne zarządzanie infrastrukturą IT.

W niniejszym dokumencie dowiesz się, w jaki sposób interfejs baramundi Proactive Hub pozwala osiągnąć właśnie tę niezbędną interoperacyjność i zapewnia zespołom IT otwartą podstawę do automatycznego raportowania zgodności, wzbogacania ITSM w czasie rzeczywistym oraz przepływów pracy między systemami – wszystko to bez zastrzeżonych łączników lub ręcznego przetwarzania danych

Treść

1	Interoperacyjność jako podstawa nowoczesnej infrastruktury IT	4
2	Czym jest baramundi Proactive Connect?	5
3	Jak działa API? – Wyjaśnienie GraphQL	6
3.1	Punkt końcowy do wszystkiego	6
3.2	Tylko te dane, które są potrzebne	6
3.3	Unikalne identyfikatory obiektów	7
3.4	Eksploracja schematu i narzędzia	7
4	Typowe przypadki użycia dla administratorów IT	8
4.1	Zautomatyzowane raportowanie zgodności	8
4.2	Panele i wizualizacje	8
4.3	Zautomatyzowane procesy wdrażania i wycofywania pracowników	8
4.4	Telemetria punktów końcowych bezpośrednio w narzędziu ITSM – baramundi Proactive Connect Wave	9
5	Uwierzytelnianie i zapytanie początkowe	11
5.1	Konfiguracja danych uwierzytelniających	11
5.2	Żądanie tokenu dostępu	11
5.3	Wyślij pierwsze zapytanie GraphQL	12
5.4	Zapoznanie się ze schematem	12
6	Bezpieczeństwo i najlepsze praktyki	13
6.1	Chroń dane uwierzytelniające	13
6.2	Obsługa tokenów	13
6.3	Optymalizuj zapytania	13
6.4	Ogranicz dostęp	13
7	Wniosek	14

©2026 baramundi software GmbH

Oświadczenia dotyczące wyposażenia i funkcji technicznych nie są wiążące i mają charakter wyłącznie informacyjny.

Zastrzegamy sobie prawo do wprowadzania zmian. Identyfikator dokumentu WP-260602

<https://www.baramundi.com/pl-pl/stopka-redakcyjna/>

1 Interoperacyjność jako podstawa nowoczesnej infrastruktury IT

Żaden system nie działa w izolacji. Systemy zgłoszeniowe, platformy monitorujące, narzędzia ITSM, rozwiązania SIEM i systemy UEM osiągają pełną wartość tylko wtedy, gdy mogą wymieniać dane i umożliwiają zespołom IT podejmowanie niezbędnych działań.

Otwarte interfejsy umożliwiają elastyczne łączenie systemów i koordynowanie zautomatyzowanych przepływów pracy bez ręcznej interwencji lub izolowanych rozwiązań punktowych. Standaryzowane technologie API oddzielają systemy i tworzą podstawę do wymiany lub aktualizacji poszczególnych komponentów bez zakłócania działania szerszej infrastruktury.

W praktyce oznacza to:

- Dane z punktów końcowych automatycznie trafiają do systemów zgłoszeń, pulpitów nawigacyjnych i raportów zgodności
- Zautomatyzowane przepływy pracy reagują w czasie rzeczywistym w różnych systemach
- Zespoły IT korzystają ze znanych narzędzi wzbogaconych o przydatne, aktualne informacje o urządzeniach
- Infrastruktura IT działa jak spójny system, a nie zbiór rozbieżnych komponentów

System baramundi Management Suite Unified Endpoint Management (UEM) oferuje **baramundi Connect**, interfejs API do wymiany danych UEM z innymi narzędziami do zarządzania. baramundi Proactive Hub, platforma chmurowa do cyfrowego doświadczenia pracowników i proaktywnego zarządzania punktami końcowymi, udostępnia **baramundi Proactive Connect**, interfejs API do danych telemetrycznych, wskaźników DEX i statusu punktów końcowych. Te uzupełniające się interfejsy API sprawiają, że cała infrastruktura baramundi jest dostępna dla systemów zewnętrznych, umożliwiając szeroki zakres funkcji zarządzania IT i automatyzacji.

baramundi Proactive Hub – inteligentny, zautomatyzowany i skalowalny

Baramundi Proactive Hub to inteligentna platforma oparta na chmurze, która gromadzi i analizuje dane dotyczące wydajności oraz bezpieczeństwa DEX we wszystkich zarządzanych punktach końcowych. Dostarcza ona zalecenia oparte na kontekście i umożliwia natychmiastowe, ukierunkowane działania naprawcze, zapewniając zespołom IT większą przejrzystość oraz możliwość skutecznego identyfikowania i rozwiązywania problemów.

2 Czym jest baramundi Proactive Connect?

baramundi Proactive Connect to oparty na GraphQL interfejs API, który zapewnia programowy dostęp do danych z baramundi Proactive Hub. Służy jako warstwa integracyjna między baramundi Proactive Hub a szerszym stosem technologicznym do zarządzania IT, udostępniając informacje o punktach końcowych tam, gdzie są potrzebne, zamiast zamykać je w oddzielnych narzędziach.

Administratorzy IT, integratorzy systemów i programiści mogą go używać do wyszukiwania informacji o punktach końcowych, integrowania ich z przepływami pracy i automatycznego przetwarzania – bezpośrednio z dowolnej aplikacji innej firmy lub własnego skryptu.

Najważniejsze funkcje w skrócie:

Funkcja	Opis
Technologia	GraphQL przez HTTPS
Uwierzytelnianie	OAuth 2.0 – poświadczenia klienta (między maszynami)
Format danych	JSON
Dostępność	W chmurze, Region UE (connect-euw.baramundi.cloud), Region Wschodnie Stany Zjednoczone (connect-use.baramundi.cloud)

API jest przeznaczone do komunikacji między usługami: zautomatyzowane systemy, skrypty i platformy integracyjne uwierzytelniają się przy użyciu własnych danych uwierzytelniających, bez konieczności interaktywnego logowania. Dzięki temu baramundi Proactive Connect nadaje się do zaplanowanych zadań automatyzacji, integracji ITSM lub niestandardowych pulpitów zarządzania.

Dane uwierzytelniające są przypisywane dla każdej integracji i zarządzane za pośrednictwem interfejsu administratora. Każdy system otrzymuje własne dane uwierzytelniające z jasno określonymi uprawnieniami. Zapewnia to szczegółową kontrolę dostępu i umożliwia dezaktywację poszczególnych integracji bez wpływu na pozostałe.

3 Jak działa API? – Wyjaśnienie GraphQL

baramundi Proactive Connect wykorzystuje GraphQL zamiast tradycyjnej architektury REST. Kluczową różnicą jest to, że to zapytanie określa, które dane są zwracane, a nie samo API.

3.1 Punkt końcowy do wszystkiego

Wszystkie żądania są wysyłane na jeden adres URL w zależności od wybranego regionu:

```
POST https://connect-euw.baramundi.cloud/eu/graphql # region UE
POST https://connect-use.baramundi.cloud/us/graphql # Region USA Est
```

Niezależnie od tego, czy chodzi o listy punktów końcowych, dane telemetryczne czy wskaźniki DEX, wszystko jest pobierane za pośrednictwem jednego punktu końcowego przy użyciu żądania POST. Nie ma wielu adresów URL do zarządzania, nie ma ścieżek zasobów z wersjami ani niespójnych formatów odpowiedzi.

3.2 Tylko te dane, które są potrzebne

Zapytanie określa dokładnie, które pola mają zostać zwrócone, co pozwala zmniejszyć ilość danych i przyspieszyć przetwarzanie:

```
{
  endpoint {
    byId(id: "...") {
      general {
        os
        lastContact
      }
    }
  }
}
```

Integracje pobierają tylko te dane, które przetwarzają – bez **pobierania nadmiarowych lub niedostatecznych danych**. Dzięki temu zapytania są zwarte i odporne na zmiany w modelu danych.

3.3 Unikalne identyfikatory obiektów

Każdy obiekt w API – punkt końcowy, środowisko i aplikacja – ma globalnie unikalny identyfikator węzła. Te stabilne identyfikatory umożliwiają niezawodne odwoływanie się do rekordów danych w wielu zapytaniach bez pomyłek spowodowanych zduplikowanymi nazwami lub zmieniającymi się identyfikatorami wewnętrznymi. Identyfikatory węzłów muszą być używane jako nieprzejrzyste ciągi znaków: należy je pobierać bezpośrednio z odpowiedzi API; nie należy ich dekodować ani konstruować samodzielnie.

3.4 Eksploracja schematu i narzędzia

Pełny schemat API – wszystkie dostępne pola, typy i opcje zapytań – można pobrać bezpośrednio. Adres URL różni się w zależności od regionu:

```
GET https://connect-euw.baramundi.cloud/eu/graphql?sdl # Region EU
GET https://connect-use.baramundi.cloud/us/graphql?sdl # Region US East
Authorization: Bearer {token}
```

Narzędzia takie jak Bruno (open source, na komputer), Postman lub GraphiQL (przeglądarkowe) ładują ten schemat i zapewniają autouzupełnianie oraz zintegrowane opisy pól podczas pisania zapytań. Jeśli nie masz wcześniejszego doświadczenia z GraphQL, jest to najszybszy sposób na rozpoczęcie pracy — schemat umożliwia przeglądanie całego API bez zewnętrznej dokumentacji.

4 Typowe przypadki użycia dla administratorów IT

4.1 Zautomatyzowane raportowanie zgodności

Scenariusz: Miesięczne raporty zgodności wymagają ręcznego eksportowania danych i czasochłonnego przetwarzania w oddzielnych narzędziach. Proces ten jest podatny na błędy i często angażuje zasoby.

Rozwiązanie: Skrypt PowerShell codziennie sprawdza aktualny status aktualizacji i wskaźniki DEX dla wszystkich punktów końcowych, a wyniki zapisuje bezpośrednio w systemie ITSM lub na pulpicie raportowym. Raport jest generowany automatycznie i zawsze odzwierciedla aktualny stan. Odchylenia od stanu docelowego są widoczne od razu, a nie dopiero podczas kolejnego ręcznego eksportu.

4.2 Panele i wizualizacje

Scenariusz: Menedżerowie IT, którzy konsolidują całą swoją infrastrukturę w scentralizowanych pulpitach menedżerskich, mogą bezpośrednio zintegrować wskaźniki DEX i status punktów końcowych z baramundi Proactive Hub.

Rozwiązanie: Dane dotyczące punktów końcowych i wskaźniki DEX są przesyłane bezpośrednio do platform wizualizacyjnych za pośrednictwem API. Zespół IT ma wszystkie istotne wskaźniki KPI w zasięgu wzroku w znanym interfejsie — skonsolidowane z danymi z innych systemów, bez ręcznego eksportowania lub kopiowania danych.

4.3 Zautomatyzowane procesy wdrażania i wycofywania pracowników

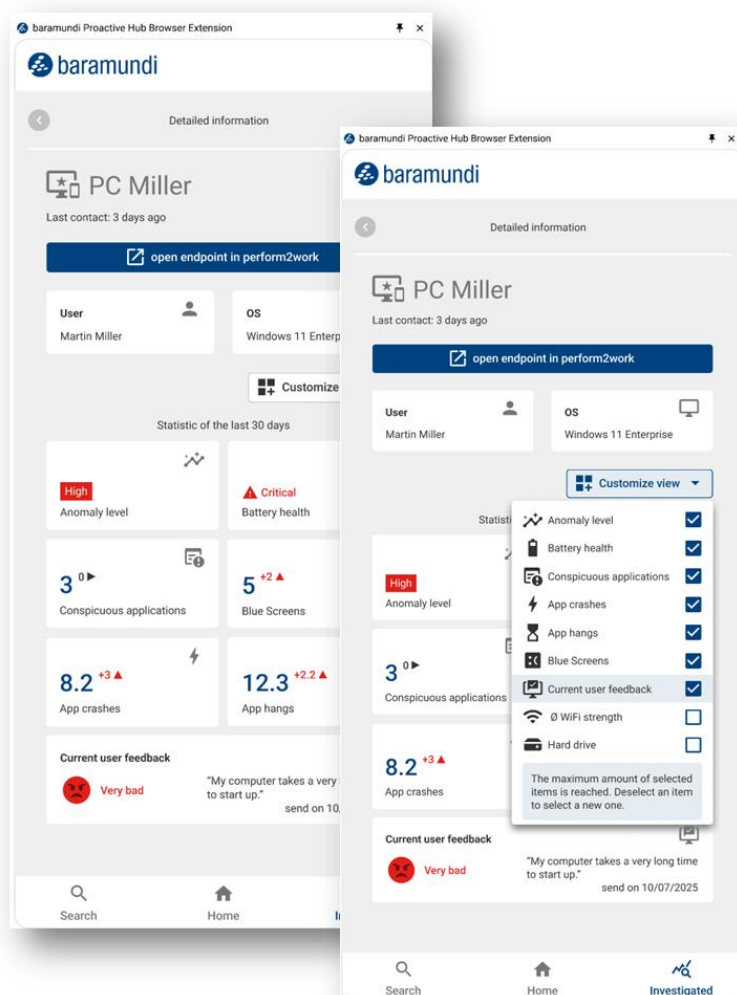
Scenariusz: Gdy pracownicy zmieniają stanowiska, stan i konfiguracja urządzeń muszą być ręcznie weryfikowane i wprowadzane do wielu systemów. Błędy pojawiają się, gdy etapy procesu są pomijane lub wykonywane z opóźnieniem.

Rozwiązanie: Automatyczne przepływy pracy pobierają aktualne dane z punktów końcowych z baramundi Proactive Hub i uruchamiają niezbędne działania następcze we wszystkich systemach. Cały proces podlega audytowi: każde działanie opiera się na zdefiniowanym wywołaniu API z wynikiem, który można zarejestrować w dzienniku.

4.4 Telemetria punktów końcowych bezpośrednio w narzędziu ITSM – baramundi Proactive Connect Wave

Scenariusz: Pracownik pomocy technicznej otwiera zgłoszenie. Narzędzie ITSM pokazuje, co zgłosił użytkownik, ale nie pokazuje, co faktycznie dzieje się na danym urządzeniu końcowym. Awarie aplikacji, problemy z siecią lub krytyczny stan dysku są rejestrowane w oddzielnym systemie. Przełączanie się między kontekstami zajmuje czas i spowalnia rozwiązywanie problemów.

Rozwiązanie: Rozszerzenie przeglądarki **baramundi Proactive Connect Wave** osadza dane z punktów końcowych na żywo z baramundi Proactive Hub bezpośrednio w internetowym narzędziu ITSM, CMDB lub narzędziu do zarządzania zasobami, bez konieczności dostosowywania narzędzia lub korzystania z drugiego ekranu.



Gdy tylko zostanie otwarte zgłoszenie lub uzyskany zostanie dostęp do punktu końcowego, odpowiednie informacje pojawiają się na pasku bocznym:

- Zawieszanie się i awarie aplikacji
- Jakość połączenia sieciowego
- Stan dysku
- Opinie użytkowników
- Wskaźniki wydajności systemu

Pracownicy pomocy technicznej mogą błyskawicznie ocenić sytuację, skuteczniej ustalać priorytety i często rozwiązywać problemy, zanim użytkownik będzie musiał zgłaszać je ponownie.

baramundi Proactive Connect Wave pokazuje, co w praktyce umożliwia otwarty interfejs API: narzędzia innych firm i rozwiązania wewnętrzne mogą bezpośrednio integrować dane z punktów końcowych – bez silosów danych i ręcznych czynności.

5 Uwierzytelnianie i zapytanie początkowe

5.1 Konfiguracja danych uwierzytelniających

Dostęp do baramundi Proactive Connect wymaga danych uwierzytelniających klienta (Client ID i Client Secret), które są udostępniane za pośrednictwem interfejsu administratora. Odpowiedzialność za to ponosi administrator baramundi. Szczegółowe instrukcje konfiguracji są dostępne w dokumentacji baramundi.

Zaleca się tworzenie oddzielnych poświadczeń dla każdej integracji z jednego prostego powodu: pozwala to na selektywne wyłączenie poszczególnych integracji bez wpływu na pozostałe.

5.2 Żądanie tokenu dostępu

Uwierzytelnianie wykorzystuje proces OAuth 2.0 Client Credentials Flow. Punkt końcowy uwierzytelniania jest taki sam dla wszystkich regionów. Poniższy przykład w PowerShell ilustruje ten proces:

```
$body = @{
    grant_type = 'client_credentials'
    client_id   = '{clientId}'
    client_secret = '{clientSecret}'
    scope       = 'https://login.baramundi.cloud/app-connect-api/.default'
}

$tokenUrl = "https://login.baramundi.cloud/login.baramundi.cloud/B2C_1A_SIGNIN/oauth2/v2.0/token"
$response = Invoke-RestMethod -Uri $tokenUrl -Method Post -Body $body
$token     = $response.access_token
```

Uwaga: Tajne klucze klienta nie powinny być nigdy przechowywane w plikach skryptów ani repozytoriach. W przypadku użytkowania produkcyjnego zaleca się przechowywanie ich w bezpiecznym magazynie (np. PowerShell Secret Management lub Azure Key Vault).

5.3 Wyślij pierwsze zapytanie GraphQL

Dzięki otrzymanemu tokenowi możesz od razu wysłać swoje pierwsze zapytanie, np. listę wszystkich dostępnych środowisk:

```
$headers = @{ Authorization = "Bearer $token" }
$graphqlUrl = 'https://connect-euw.baramundi.cloud/eu/graphql'

$query = '{ "query": "{ environment { availableToMe { nodes { id, name } } } }" }'

$result = Invoke-RestMethod -Uri $graphqlUrl -Method Post -Headers $headers `
    -ContentType 'application/json' -Body $query
$result.data.environment.availableToMe.nodes
```

Zwrócone identyfikatory środowisk służą jako punkt wyjścia dla wszystkich dalszych zapytań, takich jak pobieranie punktów końcowych w określonym środowisku.

5.4 Zapoznanie się ze schematem

Do użytku produkcyjnego zalecamy narzędzie GraphQL, takie jak Bruno (open-source, na komputer), Postman lub GraphiQL (oparte na przeglądarce). Wszystkie trzy ładują schemat bezpośrednio z API i zapewniają autouzupełnianie oraz zintegrowane opisy pól – co stanowi znaczną przewagę nad ręcznym tworzeniem zapytań.

6 Bezpieczeństwo i najlepsze praktyki

Każdy, kto wdraża integrację API, jest odpowiedzialny za zapewnienie bezpiecznego postępowania z danymi uwierzytelniającymi i wzorcami zapytań. Poniższe zalecenia mają zastosowanie niezależnie od wybranego scenariusza.

6.1 Chroń dane uwierzytelniające

- Nigdy nie przechowuj tajnych danych klienta w plikach skryptów, repozytoriach ani w wynikach logów
- Przechowuj sekrety w dedykowanym sejfie (np. PowerShell Secret Management lub Azure Key Vault)
- Regularnie zmieniaj poświadczenia dostępu i natychmiast je dezaktywuj, jeśli podejrzewasz naruszenie bezpieczeństwa
- Używaj oddzielnych poświadczeń dla każdej integracji — nigdy nie używaj jednego wspólnego klucza tajnego dla wielu systemów

6.2 Obsługa tokenów

- Tokeny dostępu wygasają po upływie określonego czasu (pole ``expires_in`` w odpowiedzi tokenu określa okres ważności w sekundach)
- Aktywnie odnawiaj tokeny przed ich wygaśnięciem — nie czekaj na błąd 401 Unauthorized
- Nie przechowuj tokenów na stałe; trzymaj je w pamięci i żądaj nowych w razie potrzeby

6.3 Optymalizuj zapytania

- Wysyłaj zapytania tylko do potrzebnych pól — GraphQL pozwala na precyzyjną kontrolę nad tym, co jest zwracane
- W przypadku dużych zbiorów danych stosuj paginację: węzły dla prostych list oraz krawędzie z kursorem dla paginacji opartej na pozycji
- Traktuj identyfikatory węzłów jako nieprzejryste ciągi znaków — nie dekoduj ich ani nie konstruuj

6.4 Ogranicz dostęp

- Utwórz oddzielne konta usługowe dla różnych scenariuszy integracji
- Ogranicz prawa dostępu do niezbędnego minimum i regularnie je weryfikuj

7 Wniosek

Systemy, które nie komunikują się ze sobą, podwajają nakład pracy. Dane z punktów końcowych widoczne tylko w systemie zarządzania są bezużyteczne dla personelu wsparcia w systemie zgłoszeń. Dane telemetryczne, które nie trafiają do przepływów pracy, nie wywołują żadnych działań.

baramundi Proactive Connect udostępnia dane z baramundi Proactive Hub systemom zewnętrznym. Dane telemetryczne, wskaźniki DEX i status punktów końcowych są dostępne za pośrednictwem interfejsu API GraphQL – zarówno dla skryptów niestandardowych, aplikacji innych firm, jak i specjalistycznych rozwiązań, takich jak baramundi Proactive Connect Wave.

W połączeniu z bConnect dla baramundi Management Suite zapewnia to kompletną podstawę API: dwa interfejsy, które wzajemnie się uzupełniają i otwierają całą infrastrukturę baramundi na systemy zewnętrzne.

Dla zespołów IT oznacza to:

- Mniej pracy ręcznej dzięki przepływowi pracy opartym na API
- Krótszy czas reakcji dzięki bezpośredniej analizie danych telemetrycznych
- Lepsze podejmowanie decyzji dzięki integracji z istniejącymi pulpitami nawigacyjnymi i systemami ITSM
- Architektura gotową na przyszłość, zbudowaną w oparciu o otwarte, standardowe technologie (GraphQL / OAuth 2.0)
- Skalowalność: każda nowa integracja opiera się na tej samej wspólnej podstawie

Więcej informacji, dokumentacja i przykładowe skrypty:

github.com/baramundisoftware/Proactive-Connect

Zespoły IT rozważające wdrożenie Proactive Hub mogą poprosić o bezpłatną 30-dniową pełną wersję lub wdrożenie proof-of-concept we własnej sieci, aby osobiście przekonać się o korzyściach.

Wypróbuj pełną wersję już teraz: [baramundi Proactive Hub](#)

Napisz do nas! *Czekamy na Ciebie!*



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+49 821 56708-390
request@baramundi.com

Making IT Admins Smile