

baramundi Proactive Connect API

*Gezielte Integration von Endpunktdaten –
Interoperabilität als Grundlage
moderner IT-Infrastrukturen*

Executive Summary

IT-Umgebungen leben von dem Austausch von Daten – ohne manuellen Eingriff – über verschiedene Tools hinweg. Der baramundi Proactive Hub sammelt und analysiert Performance- und Stabilitäts-Metriken sowie Security-Indikatoren und ermöglicht so ein proaktives Management der IT-Infrastruktur.

In diesem Dokument erfahren Sie, wie Sie mit der Schnittstelle des baramundi Proactive Hub genau diese notwendige Interoperabilität erreichen und IT-Teams eine offene Grundlage für automatisierte Compliance-Berichte, Echtzeit-ITSM-Anreicherung und systemübergreifende Workflows erhalten können – ganz ohne proprietäre Konnektoren oder manuelle Datenbearbeitung.

Inhalt

1	Interoperabilität als Grundlage moderner IT-Infrastrukturen	4
2	Was ist baramundi Proactive Connect?	5
3	Wie funktioniert die API? – GraphQL einfach erklärt	6
3.1	Ein Endpunkt für alles	6
3.2	Nur die Daten, die wirklich gebraucht werden	6
3.3	Eindeutige Objekt-IDs	7
3.4	Schema-Exploration und Tooling	7
4	Typische Anwendungsfälle für IT-Admins	8
4.1	Automatisiertes Compliance-Reporting	8
4.2	Dashboards und Visualisierungen	8
4.3	Automatisierte Onboarding- und Offboarding-Prozesse	8
4.4	Direkte Verbindung zum ITSM-Tool – baramundi Proactive Connect Wave	9
5	Authentifizierung und erste Abfrage	11
5.1	Zugangsdaten einrichten	11
5.2	Access Token anfordern	11
5.3	Erste GraphQL-Abfrage senden	12
5.4	Schema erkunden	12
6	Sicherheit und Best Practices	13
6.1	Zugangsdaten schützen	13
6.2	Token-Handling	13
6.3	Abfragen optimieren	13
6.4	Zugriff einschränken	13
7	Fazit	14

© 2026 baramundi software GmbH. Statements about equipment and technical functionalities are non-binding and are for information purposes only.

We reserve the right to make changes. Doc ID WP-260602

<https://www.baramundi.com/de-de/disclaimer>

1 Interoperabilität als Grundlage moderner IT-Infrastrukturen

Kein System arbeitet allein. Ticketsysteme, Monitoring-Plattformen, ITSM-Tools, SIEM-Lösungen und UEM-Systeme erbringen ihren vollen Wert erst dann, wenn sie miteinander kommunizieren können – wenn Daten dort verfügbar sind, wo Entscheidungen getroffen und Aktionen ausgeführt werden.

Offene Schnittstellen sind dafür die Voraussetzung. Sie ermöglichen es, Systeme flexibel zu verbinden, Workflows zu automatisieren und Informationen kontextbezogen bereitzustellen – ohne manuelle Umwege oder proprietäre Insellösungen. Standardisierte API-Technologien entkoppeln Systeme voneinander und schaffen die Grundlage dafür, dass einzelne Komponenten ausgetauscht oder erweitert werden können, ohne den gesamten Verbund zu gefährden.

Was das in der Praxis bedeutet:

- Endpoint-Daten fließen automatisch in Ticketsysteme, Dashboards und Compliance-Berichte
- Automatisierte Workflows reagieren auf Ereignisse in Echtzeit – systemübergreifend
- IT-Teams arbeiten in ihren gewohnten Werkzeugen, angereichert mit aktuellen Geräteinformationen
- Die gesamte IT-Infrastruktur verhält sich wie ein kohärentes System statt wie eine Sammlung von Datensilos

Die baramundi Management Suite bietet mit **baramundi Connect** eine API-Schnittstelle für UEM-Daten. baramundi Proactive Hub – die Cloud-Plattform für Digital Employee Experience und proaktives Endpoint Management – ergänzt dieses Fundament mit **baramundi Proactive Connect** um eine eigene API-Schnittstelle für Telemetriedaten, DEX-Metriken und Endpoint-Status. Beide Schnittstellen ergänzen sich und machen die gesamte baramundi-Infrastruktur für externe Systeme zugänglich.

Der baramundi Proactive Hub – intelligent, automatisiert und skalierbar

Der baramundi Proactive Hub ist eine cloud-basierte Plattform für modernes und schlankes Endpoint Management. Er bündelt und wertet DEX-Performance- sowie Security-Daten intelligent aus, leitet kontextbezogene Empfehlungen ab und ermöglicht eine unmittelbare Remediation. Durch die Kombination aus Insights, Guidance und Action erhalten IT-Teams nicht nur volle Transparenz, sondern auch die Fähigkeit, Probleme frühzeitig zu erkennen und gezielt zu lösen.

2 Was ist baramundi Proactive Connect?

baramundi Proactive Connect ist eine GraphQL-basierte API, die den programmatischen Zugriff auf Daten aus baramundi Proactive Hub ermöglicht. IT-Admins, Systemintegratoren und Entwickler können damit Endpoint-Informationen abfragen, in eigene Workflows einbinden und automatisiert weiterverarbeiten – direkt aus jeder Drittanwendung oder einem eigenen Skript heraus.

Kernmerkmale auf einen Blick:

Merkmal	Beschreibung
Technologie	GraphQL über HTTPS
Authentifizierung	OAuth 2.0 Client Credentials (machine-to-machine)
Datenformat	JSON
Verfügbarkeit	Cloud-basiert, Region EU (connect-euw.baramundi.cloud), Region US East (connect-use.baramundi.cloud)

Die API ist für service-to-service-Kommunikation ausgelegt: Automatisierte Systeme, Skripte und Integrationsplattformen authentifizieren sich mit eigenen Zugangsdaten – kein interaktiver Login erforderlich. Das macht baramundi Proactive Connect geeignet für geplante Automatisierungsaufgaben, ITSM-Integrationen oder eigene Management-Dashboards.

Zugangsdaten werden pro Integration vergeben und über die Administrationsoberfläche verwaltet. Unterschiedliche Systeme erhalten separate Credentials mit klar definierten Berechtigungen – der Zugriff bleibt damit granular steuerbar und einzelne Integrationen lassen sich jederzeit deaktivieren, ohne andere zu beeinflussen.

3 Wie funktioniert die API? – GraphQL einfach erklärt

baramundi Proactive Connect nutzt GraphQL statt klassischer REST-Architektur. Der wesentliche Unterschied: Nicht die API bestimmt, welche Daten zurückgegeben werden – sondern die Abfrage selbst.

3.1 Ein Endpunkt für alles

Alle Anfragen gehen an einen einzigen URL – je nach gebuchter Region:

```
POST https://connect-euw.baramundi.cloud/eu/graphql # Region EU
POST https://connect-use.baramundi.cloud/us/graphql # Region US East
```

Ob Endpoint-Listen, Telemetriedaten oder DEX-Metriken – alles wird über diesen einen Endpunkt per POST-Anfrage abgerufen. Es gibt keine Vielzahl von URLs zu verwalten, keine versionierten Ressourcenpfade, keine inkonsistenten Rückgabeformate.

3.2 Nur die Daten, die wirklich gebraucht werden

Die Abfrage beschreibt exakt, welche Felder zurückgegeben werden sollen. Das reduziert Datenvolumen und beschleunigt die Verarbeitung:

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

Integrationen fordern nur das an, was sie tatsächlich verarbeiten – kein **Overfetching**, kein **Underfetching**. Das hält Abfragen schlank und macht sie robuster gegenüber Änderungen am Datenmodell.

3.3 Eindeutige Objekt-IDs

Jedes Objekt in der API – Endpoint, Umgebung, Anwendung – besitzt eine global eindeutige Node-ID. Diese stabilen Bezeichner ermöglichen es, Datensätze zuverlässig über mehrere Abfragen hinweg zu referenzieren, ohne Verwechslungen durch doppelte Namen oder wechselnde interne IDs. Node-IDs sind als opaque Strings zu verwenden: direkt aus API-Antworten übernehmen, nicht dekodieren oder selbst konstruieren.

3.4 Schema-Exploration und Tooling

Das vollständige API-Schema – alle verfügbaren Felder, Typen und Abfragemöglichkeiten – lässt sich direkt abrufen. Die URL variiert je nach Region:

```
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}
```

Tools wie Bruno (Open-Source, Desktop), Postman oder GraphiQL (browser-basiert) laden dieses Schema und bieten Autovervollständigung sowie integrierte Felddesreibungen direkt beim Schreiben von Abfragen. Wer noch keine Erfahrung mit GraphQL hat, findet hier den schnellsten Einstieg – das Schema macht die gesamte API explorierbar, ohne externe Dokumentation zu benötigen.

4 Typische Anwendungsfälle für IT-Admins

4.1 Automatisiertes Compliance-Reporting

Problem: Monatliche Compliance-Berichte erfordern manuelle Datenexporte und aufwendige Aufbereitung in separaten Tools. Der Prozess ist fehleranfällig und bindet regelmäßig Kapazitäten.

Lösung: Ein PowerShell-Skript fragt täglich den aktuellen Update-Status und DEX-Metriken aller Endpoints ab und schreibt die Ergebnisse direkt in das ITSM-System oder ein Reporting-Dashboard. Der Bericht entsteht automatisch und spiegelt stets den aktuellen Stand wider. Abweichungen vom Soll-Zustand werden sofort sichtbar, nicht erst beim nächsten manuellen Export.

4.2 Dashboards und Visualisierungen

Szenario: IT-Verantwortliche, die ihre gesamte Infrastruktur in zentralen Management-Dashboards konsolidieren, können DEX-Metriken und Endpoint-Status aus baramundi Proactive Hub direkt einbinden.

Lösung: Endpoint-Daten und DEX-Metriken werden per API direkt an Visualisierungsplattformen übergeben. Das IT-Team hat alle relevanten KPIs in der gewohnten Oberfläche im Blick – konsolidiert mit Daten aus anderen Systemen, ohne manuelle Exporte oder Datenkopien.

4.3 Automatisierte Onboarding- und Offboarding-Prozesse

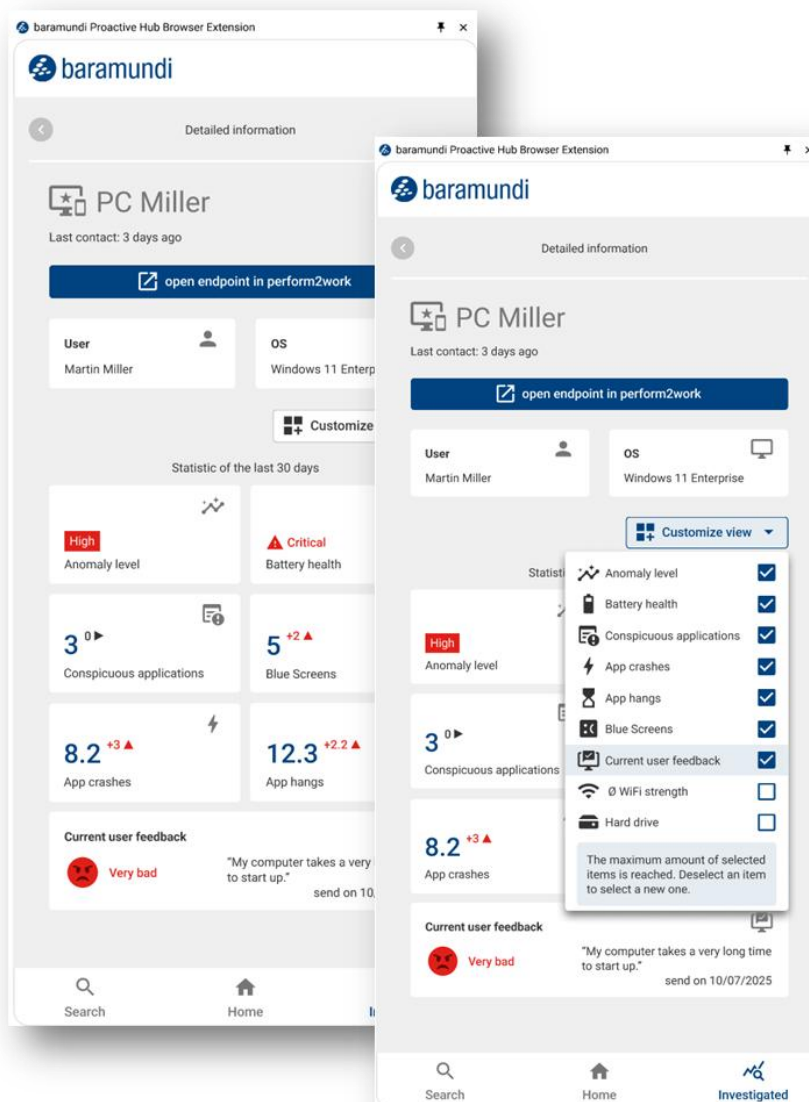
Problem: Bei Mitarbeiterwechseln müssen Gerätestatus und Konfigurationszustand manuell geprüft und in mehrere Systeme eingetragen werden. Fehler entstehen, weil Prozessschritte übersehen oder verspätet ausgeführt werden.

Lösung: Automatisierungsworkflows greifen auf aktuelle Endpoint-Daten aus baramundi Proactive Hub zu und stoßen die notwendigen Folgeaktionen systemübergreifend an. Der gesamte Prozess wird auditierbar: Jede Aktion basiert auf einem definierten API-Aufruf mit protokollierbarem Ergebnis.

4.4 Direkte Verbindung zum ITSM-Tool – baramundi Proactive Connect Wave

Situation: Ein Support-Mitarbeiter öffnet ein Ticket. Das ITSM-Tool zeigt, was der User gemeldet hat – nicht aber, was auf dem betroffenen Endpoint tatsächlich los ist. App-Crashes, Netzwerkprobleme oder ein kritischer Disk-Health-Status sind in einem separaten System hinterlegt. Der Kontextwechsel kostet Zeit und verlangsamt die Problemlösung.

baramundi Proactive Connect Wave löst genau dieses Problem: Die Browser-Extension bettet Live-Endpoint-Daten aus baramundi Proactive Hub direkt in das webbasierte ITSM-, CMDB- oder Asset-Management-Tool ein – ohne Anpassung am jeweiligen Tool, ohne zweiten Bildschirm.



Sobald ein Ticket geöffnet oder ein Endpoint aufgerufen wird, erscheinen die relevanten Informationen direkt in der Sidebar:

- App-Hangs und -Crashes
- Netzwerkverbindungsqualität
- Disk-Health
- User Feedback
- Systemleistungsindikatoren

Der Support-Mitarbeiter kann eine Situation auf einen Blick einschätzen, Prioritäten gezielter setzen und Probleme häufig beheben, bevor der User ein zweites Mal nachfragen muss.

baramundi Proactive Connect Wave zeigt, was eine offene API in der Praxis ermöglicht: Drittanbieter-Tools und eigene Lösungen binden Endpoint-Daten direkt ein – ohne Medienbruch, ohne manuelle Schritte.

5 Authentifizierung und erste Abfrage

5.1 Zugangsdaten einrichten

Der Zugriff auf baramundi Proactive Connect erfordert Client-Zugangsdaten (Client ID und Client Secret), die über die Administrationsoberfläche bereitgestellt werden. Zuständig dafür ist der jeweilige baramundi-Administrator. Detaillierte Einrichtungshinweise finden sich in der baramundi-Dokumentation.

Pro Integration eigene Credentials anzulegen empfiehlt sich aus einem einfachen Grund: Einzelne Integrationen lassen sich so gezielt deaktivieren, ohne andere zu beeinflussen.

5.2 Access Token anfordern

Die Authentifizierung erfolgt über den OAuth 2.0 Client Credentials Flow. Der Authentifizierungs-Endpunkt ist für alle Regionen identisch. Das folgende PowerShell-Beispiel zeigt den Ablauf:

```
$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
```

Hinweis: Client-Secrets gehören nie in Skriptdateien oder Repositories. Für den Produktionseinsatz empfiehlt sich die Ablage in einem sicheren Vault (z.B. PowerShell SecretManagement oder Azure Key Vault).

5.3 Erste GraphQL-Abfrage senden

Mit dem erhaltenen Token lässt sich sofort die erste Abfrage senden – zum Beispiel eine Liste aller verfügbaren Umgebungen:

```
$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
```

Die zurückgegebenen Umgebungs-IDs dienen als Ausgangspunkt für alle weiteren Abfragen – etwa zum Abrufen von Endpoints innerhalb einer bestimmten Umgebung.

5.4 Schema erkunden

Für den produktiven Einsatz empfiehlt sich ein GraphQL-Tool wie Bruno (Open-Source, Desktop), Postman oder GraphiQL (browser-basiert). Alle drei laden das Schema direkt von der API und bieten Autovervollständigung sowie integrierte Feldbeschreibungen – ein erheblicher Vorteil gegenüber dem manuellen Aufbau von Abfragen.

6 Sicherheit und Best Practices

Wer eine API-Integration in Betrieb nimmt, trägt Verantwortung für den sicheren Umgang mit Zugangsdaten und Abfragemustern. Die folgenden Empfehlungen gelten unabhängig vom gewählten Szenario.

6.1 Zugangsdaten schützen

- Client Secret niemals in Skriptdateien, Repositories oder Log-Ausgaben speichern
- Secrets in einem dedizierten Vault ablegen (z.B. PowerShell SecretManagement oder Azure Key Vault)
- Zugangsdaten regelmäßig rotieren und bei Verdacht auf Kompromittierung sofort deaktivieren
- Pro Integration separate Credentials verwenden – nie ein gemeinsames Secret für mehrere Systeme

6.2 Token-Handling

- Access Tokens laufen nach begrenzter Zeit ab (expires_in im Token-Response gibt die Gültigkeitsdauer in Sekunden an)
- Token proaktiv erneuern, bevor sie ablaufen – nicht erst nach einem 401 Unauthorized-Fehler
- Tokens nicht dauerhaft speichern; im Arbeitsspeicher halten und bei Bedarf neu anfordern

6.3 Abfragen optimieren

- Nur die tatsächlich benötigten Felder abfragen – GraphQL erlaubt präzise Kontrolle darüber, was zurückgegeben wird
- Bei großen Datensätzen Paginierung nutzen: nodes für einfache Listen, edges mit cursor für positionsgenaue Paginierung
- Node-IDs als opaque Strings behandeln – nicht dekodieren oder selbst konstruieren

6.4 Zugriff einschränken

- Separate Service-Accounts für unterschiedliche Integrations-Szenarien anlegen
- Zugriffsrechte auf das notwendige Minimum beschränken und regelmäßig überprüfen

7 Fazit

Systeme, die nicht miteinander sprechen, verdoppeln Aufwand. Endpoint-Daten, die nur im Managementsystem sichtbar sind, helfen dem Support-Mitarbeiter im Ticketsystem nicht weiter. Telemetriedaten, die nicht in Workflows fließen, lösen keine Maßnahmen aus.

baramundi Proactive Connect macht die Daten aus baramundi Proactive Hub für externe Systeme zugänglich: Telemetriedaten, DEX-Metriken und Endpoint-Status stehen per GraphQL-API bereit – für eigene Skripte, Drittanwendungen und spezialisierte Lösungen wie baramundi Proactive Connect Wave gleichermaßen.

Gemeinsam mit bConnect für die baramundi Management Suite steht damit ein vollständiges API-Fundament zur Verfügung: zwei Schnittstellen, die sich ergänzen und die gesamte baramundi-Infrastruktur für externe Systeme öffnen.

Das bedeutet für IT-Teams:

- Weniger manuelle Arbeit durch API-gestützte Workflows
- Kürzere Reaktionszeiten durch direkte Auswertung von Telemetriedaten
- Bessere Entscheidungsgrundlagen durch Integration in bestehende Dashboards und ITSM-Systeme
- Zukunftssicher durch offene, standardisierte Technologien (GraphQL / OAuth 2.0)
- Skalierbar: Neue Integrationen bauen auf demselben Fundament auf

Weitere Informationen, Dokumentation und Beispielskripte:

github.com/baramundisoftware/Proactive-Connect

IT-Teams, die den Proactive Hub in Betracht ziehen, können unsere kostenlose 30-Tage-Vollversion oder eine Proof-of-Concept-Bereitstellung in ihrem eigenen Netzwerk anfordern, und sich selbst von den Vorteilen überzeugen.

Jetzt Vollversion testen: [baramundi Proactive Hub](#)

Kontaktieren Sie uns. *Wir freuen uns auf Sie!*



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



+43 1 928 0136 0010
request@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



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



+49 821 56708-390
request@baramundi.com



Making IT Admins Smile