

baramundi Proactive Connect API

*Targeted integration of endpoint data –
interoperability as the foundation of
modern IT infrastructures*

Executive Summary

IT environments thrive on the exchange of data—without manual intervention—across various tools. The baramundi Proactive Hub collects and analyzes performance and stability metrics as well as security indicators, enabling proactive management of the IT infrastructure.

In this document, you will learn how the baramundi Proactive Hub's interface enables you to achieve precisely this necessary interoperability and provide IT teams with an open foundation for automated compliance reporting, real-time ITSM enrichment, and cross-system workflows—all without proprietary connectors or manual data processing

Content

1	Interoperability as the foundation of modern IT infrastructure.....	4
2	What is baramundi Proactive Connect?	5
3	How does the API work? – GraphQL explained.....	6
3.1	One endpoint for everything	6
3.2	Only the data that is needed.....	6
3.3	Unique Object IDs	7
3.4	Schema Exploration and Tooling.....	7
4	Typical use cases for IT admins	8
4.1	Automated compliance reporting	8
4.2	Dashboards and Visualizations	8
4.3	Automated onboarding and offboarding processes	8
4.4	Endpoint telemetry in the ITSM tool – baramundi Proactive Connect Wave.....	9
5	Authentication and Initial Query.....	11
5.1	Set up access credentials	11
5.2	Request an access token	11
5.3	Send the first GraphQL query	12
5.4	Exploring the Schema	12
6	Security and Best Practices.....	13
6.1	Protect access credentials.....	13
6.2	Token Handling.....	13
6.3	Optimize queries.....	13
6.4	Restrict access	13
7	Conclusion	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/en-us/disclaimer>

1 Interoperability as the foundation of modern IT infrastructure

No system works in isolation. Ticketing systems, monitoring platforms, ITSM tools, SIEM solutions, and UEM systems deliver their full value only when they can share data and enable IT teams to take necessary actions.

Open interfaces enable systems to connect flexibly and coordinate automated workflows without manual intervention or siloed point solutions. Standardized API technologies decouple systems and create a foundation for replacing or upgrading individual components without disrupting the broader infrastructure.

In practice, this means:

- Endpoint data flows automatically into ticketing systems, dashboards, and compliance reports
- Automated workflows respond in real time across systems
- IT teams use familiar tools enriched with actionable, up-to-date device information
- IT infrastructure behaves like a coherent system rather than a collection of disparate components

The baramundi Management Suite Unified Endpoint Management (UEM) system offers **baramundi Connect**, an API for exchanging UEM data with other management tools. baramundi Proactive Hub, the cloud platform for Digital Employee Experience and proactive endpoint management, provides **baramundi Proactive Connect**, an API for telemetry data, DEX metrics, and endpoint status. These complementary APIs make the entire baramundi infrastructure accessible to external systems, enabling a comprehensive range of IT management capabilities and automations.

The baramundi Proactive Hub – intelligent, automated, and scalable

The baramundi Proactive Hub is an intelligent cloud-based platform that collects and analyzes DEX performance and security data across managed endpoints. It provides context-based recommendations and enables immediate, targeted remediation, giving IT teams increased transparency and the ability to identify and resolve issues effectively.

2 What is baramundi Proactive Connect?

baramundi Proactive Connect is a GraphQL-based API that provides programmatic access to data from the baramundi Proactive Hub. It serves as the integration layer between the baramundi Proactive Hub and the broader IT management tech stack, making endpoint intelligence available where it's needed rather than locked inside separate tools.

IT admins, system integrators, and developers can use it to query endpoint information, integrate it into workflows, and process it automatically—directly from any third-party application or their own script.

Key features at a glance:

Feature	Description
Technology	GraphQL over HTTPS
Authentication	OAuth 2.0 Client Credentials (machine-to-machine)
Data Format	JSON
Availability	Cloud-based, Region EU (connect-euw.baramundi.cloud), Region US East (connect-use.baramundi.cloud)

The API is designed for service-to-service communication: Automated systems, scripts, and integration platforms authenticate with their own credentials, with no interactive login required. This makes baramundi Proactive Connect suitable for scheduled automation tasks, ITSM integrations, or custom management dashboards.

Credentials are assigned per integration and managed through the administrator interface. Each system receives its own credentials with clearly defined permissions. This ensures granular access control and allows deactivation of individual integrations without affecting others.

3 How does the API work? – GraphQL explained

baramundi Proactive Connect uses GraphQL instead of a traditional REST architecture. The key difference is that the query determines which data is returned, not the API itself.

3.1 One endpoint for everything

All requests are sent to a single URL based on the region selected:

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

Whether it's endpoint lists, telemetry data, or DEX metrics, everything is retrieved via a single endpoint using a POST request. There are no multiple URLs to manage, no versioned resource paths, and no inconsistent response formats.

3.2 Only the data that is needed

The query specifies exactly which fields to return to reduce data volume and speed processing:

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

Integrations request only what they process—**no overfetching or underfetching**. This keeps queries lean and resilient to changes in the data model.

3.3 Unique Object IDs

Every object in the API—endpoint, environment, and application—has a globally unique Node ID. These stable identifiers make it possible to reliably reference data records across multiple queries without confusion caused by duplicate names or changing internal IDs. Node IDs must be used as opaque strings: take them directly from API responses; do not decode or construct them yourself.

3.4 Schema Exploration and Tooling

The complete API schema—all available fields, types, and query options—can be retrieved directly. The URL varies by 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 such as Bruno (open-source, desktop), Postman, or GraphiQL (browser-based) load this schema and provide autocomplete and integrated field descriptions as you write queries. If you have no prior experience with GraphQL, this is the fastest way to get started—the schema makes the entire API explorable without external documentation.

4 Typical use cases for IT admins

4.1 Automated compliance reporting

Scenario: Monthly compliance reports require manual data exports and time-consuming processing in separate tools. The process is error-prone and frequently ties up resources.

Solution: A PowerShell script queries the current update status and DEX metrics for all endpoints daily and writes the results directly to the ITSM system or a reporting dashboard. The report is generated automatically and always reflects the current status. Deviations from the target state are visible immediately, not just during the next manual export.

4.2 Dashboards and Visualizations

Scenario: IT managers who consolidate their entire infrastructure into centralized management dashboards can directly integrate DEX metrics and endpoint status from the baramundi Proactive Hub.

Solution: Endpoint data and DEX metrics are sent directly to visualization platforms via the API. The IT team has all relevant KPIs at a glance in the familiar interface—consolidated with data from other systems, without manual exports or data copies.

4.3 Automated onboarding and offboarding processes

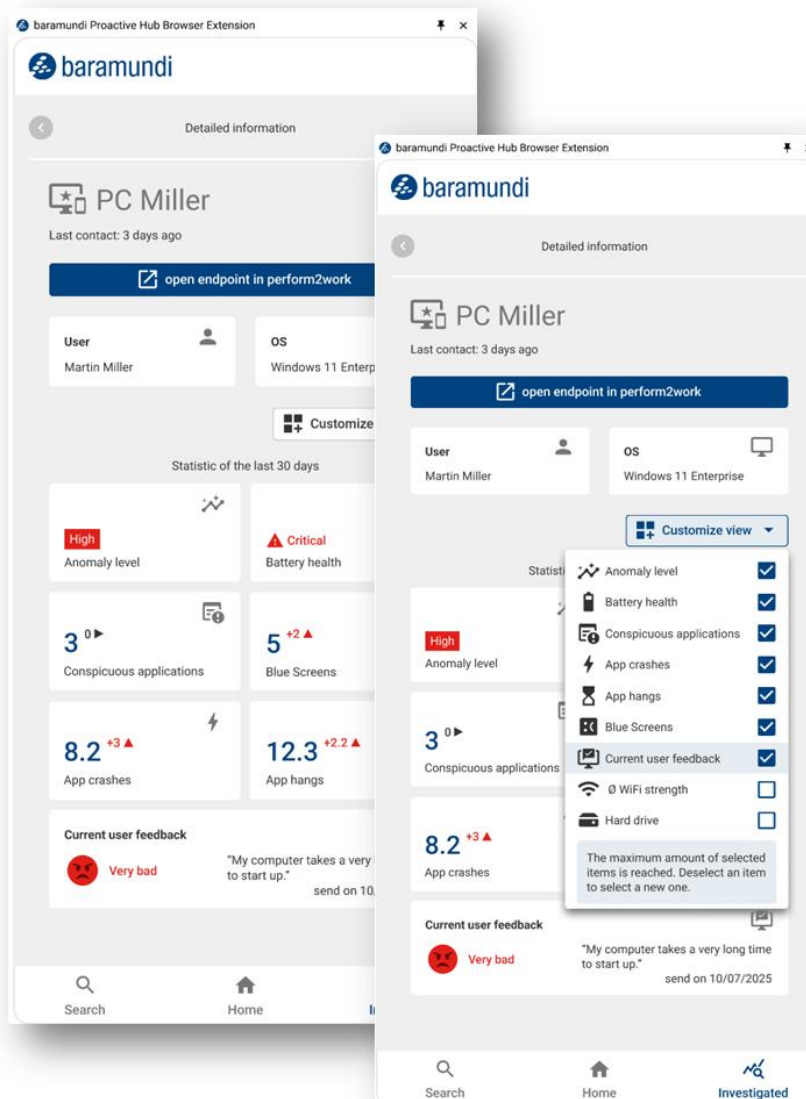
Scenario: When employees change roles, device status and configuration must be manually verified and entered into multiple systems. Errors occur when process steps are overlooked or executed late.

Solution: Automation workflows retrieve current endpoint data from the baramundi Proactive Hub and trigger the necessary follow-up actions across systems. The entire process is auditable: every action is based on a defined API call with a loggable result.

4.4 Endpoint telemetry in the ITSM tool – baramundi Proactive Connect Wave

Scenario: A support agent opens a ticket. The ITSM tool shows what the user reported, but not what is actually happening on the affected endpoint. App crashes, network issues, or critical disk health status are logged in a separate system. Switching contexts takes time and slows problem resolution.

Solution: The **baramundi Proactive Connect Wave** browser extension embeds live endpoint data from baramundi Proactive Hub directly into the web-based ITSM, CMDB, or asset management tool, without requiring any customization of the tool or a second screen.



As soon as a ticket is opened or an endpoint is accessed, the relevant information appears in the sidebar:

- App freezes and crashes
- Network connection quality
- Disk health
- User feedback
- System performance indicators

Support staff can assess a situation at a glance, set priorities more effectively, and often resolve issues before the user needs to follow up.

baramundi Proactive Connect Wave demonstrates what an open API enables in practice: third-party tools and in-house solutions can integrate endpoint data directly—without data silos or manual steps.

5 Authentication and Initial Query

5.1 Set up access credentials

Access to baramundi Proactive Connect requires client credentials (Client ID and Client Secret), which are provided via the administrator interface. The respective baramundi administrator is responsible for this. Detailed setup instructions are available in the baramundi documentation.

Creating separate credentials for each integration is recommended for one simple reason: it allows individual integrations to be deactivated selectively without affecting the others.

5.2 Request an access token

Authentication uses the OAuth 2.0 Client Credentials Flow. The authentication endpoint is the same for all regions. The following PowerShell example demonstrates the process:

```
$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
```

Note: Client secrets should never be stored in script files or repositories. For production use, it is recommended to store them in a secure vault (e.g., PowerShell Secret Management or Azure Key Vault).

5.3 Send the first GraphQL query

With the token you received, you can immediately send your first query, e.g., a list of all available environments:

```
$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
```

The returned environment IDs serve as a starting point for all further queries, such as retrieving endpoints within a specific environment.

5.4 Exploring the Schema

For production use, we recommend a GraphQL tool such as Bruno (open-source, desktop), Postman, or GraphiQL (browser-based). All three load the schema directly from the API and provide autocomplete and integrated field descriptions—a significant advantage over manually building queries.

6 Security and Best Practices

Anyone who implements an API integration is responsible for ensuring the secure handling of access credentials and query patterns. The following recommendations apply regardless of the chosen scenario.

6.1 Protect access credentials

- Never store client secrets in script files, repositories, or log outputs
- Store secrets in a dedicated vault (e.g., PowerShell Secret Management or Azure Key Vault)
- Rotate access credentials regularly and deactivate them immediately if compromise is suspected
- Use separate credentials for each integration—never use a single shared secret for multiple systems

6.2 Token Handling

- Access tokens expire after a limited time (the `expires_in` field in the token response specifies the validity period in seconds)`
- Proactively renew tokens before they expire—do not wait for a 401 Unauthorized error
- Do not store tokens permanently; keep them in memory and request new ones as needed

6.3 Optimize queries

- Only query the fields that are needed—GraphQL allows precise control over what is returned
- Use pagination for large datasets: nodes for simple lists, and edges with a cursor for position-specific pagination
- Treat node IDs as opaque strings—do not decode or construct them

6.4 Restrict access

- Create separate service accounts for different integration scenarios
- Limit access rights to the minimum necessary and review them regularly

7 Conclusion

Systems that don't communicate with each other double the effort. Endpoint data visible only in the management system is of no use to support staff in the ticketing system. Telemetry data that doesn't flow into workflows doesn't trigger any actions.

baramundi Proactive Connect makes data from baramundi Proactive Hub accessible to external systems. Telemetry data, DEX metrics, and endpoint status are available via the GraphQL API— for custom scripts, third-party applications, and specialized solutions like baramundi Proactive Connect Wave alike.

Together with bConnect for the baramundi Management Suite, this provides a complete API foundation: two interfaces that complement each other and open up the entire baramundi infrastructure to external systems.

For IT teams, this means:

- Less manual work thanks to API-driven workflows
- Shorter response times through direct analysis of telemetry data
- Better decision-making through integration into existing dashboards and ITSM systems
- A future-ready architecture built with open, standardized technologies (GraphQL / OAuth 2.0)
- Scalable: each new integration builds on the same shared foundation

Further information, documentation, and sample scripts:

github.com/baramundisoftware/Proactive-Connect

IT teams considering the Proactive Hub can request our free 30-day full version or a proof-of-concept deployment on their own network to see the benefits for themselves.

Try the full version now: [baramundi Proactive Hub](#)

Get in Touch!

We are looking forward to meeting you!



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