

API baramundi Proactive Connect

*Integrazione mirata dei dati degli endpoint –
L'interoperabilità come fondamento delle
moderne infrastrutture IT*

Sintesi

Gli ambienti IT prosperano grazie allo scambio di dati – senza intervento manuale – tra vari strumenti. Il baramundi Proactive Hub raccoglie e analizza metriche di prestazioni e stabilità, nonché indicatori di sicurezza, consentendo una gestione proattiva dell'infrastruttura IT.

In questo documento scoprirai come l'interfaccia di baramundi Proactive Hub ti consenta di ottenere proprio questa necessaria interoperabilità e di fornire ai team IT una base aperta per la reportistica automatizzata sulla conformità, l'arricchimento ITSM in tempo reale e i flussi di lavoro tra sistemi, il tutto senza connettori proprietari o elaborazione manuale dei dati

Contenuti

1	L'interoperabilità come fondamento dell'infrastruttura IT moderna	4
2	Cos'è baramundi Proactive Connect?	5
3	Come funziona l'API? – Spiegazione di GraphQL.....	6
3.1	Un unico endpoint per tutto	6
3.2	Solo i dati necessari	6
3.3	ID oggetto univoci	7
3.4	Esplorazione dello schema e strumenti.....	7
4	Casi d'uso tipici per gli amministratori IT	8
4.1	Reportistica automatizzata sulla conformità.....	8
4.2	Dashboard e visualizzazioni.....	8
4.3	Processi automatizzati di onboarding e offboarding	8
4.4	Telemetria degli endpoint direttamente nello strumento ITSM – baramundi Proactive Connect Wave	9
5	Autenticazione e query iniziale	11
5.1	Configurazione delle credenziali di accesso	11
5.2	Richiesta di un token di accesso	11
5.3	Invia la prima query GraphQL	12
5.4	Esplorazione dello schema	12
6	Sicurezza e best practice	13
6.1	Proteggere le credenziali di accesso	13
6.2	Gestione dei token	13
6.3	Ottimizzare le query	13
6.4	Limita l'accesso	13
7	Conclusione	14

©2026 baramundi software GmbH

Le dichiarazioni relative alle apparecchiature e alle funzionalità tecniche non sono vincolanti e hanno solo scopo informativo.

Ci riserviamo il diritto di apportare modifiche. ID documento WP-260602

<https://www.baramundi.com/it-it/note-legali/>

1 L'interoperabilità come fondamento dell'infrastruttura IT moderna

Nessun sistema funziona in modo isolato. I sistemi di ticketing, le piattaforme di monitoraggio, gli strumenti ITSM, le soluzioni SIEM e i sistemi Unified Endpoint Management offrono il loro pieno valore solo quando possono condividere i dati e consentire ai team IT di intraprendere le azioni necessarie.

Le interfacce aperte consentono ai sistemi di connettersi in modo flessibile e di coordinare flussi di lavoro automatizzati senza interventi manuali o soluzioni puntuali isolate. Le tecnologie API standardizzate separano i sistemi e creano una base per la sostituzione o l'aggiornamento di singoli componenti senza interrompere l'infrastruttura più ampia.

In pratica, ciò significa:

- I dati degli endpoint confluiscono automaticamente nei sistemi di ticketing, nei dashboard e nei report di conformità
- I flussi di lavoro automatizzati rispondono in tempo reale su tutti i sistemi
- I team IT utilizzano strumenti familiari arricchiti da informazioni sui dispositivi aggiornate e utilizzabili
- L'infrastruttura IT si comporta come un sistema coerente piuttosto che come un insieme di componenti disparati

Il sistema Unified Endpoint Management (UEM) della baramundi Management Suite offre **baramundi Connect**, un'API per lo scambio di dati UEM con altri strumenti di gestione. baramundi Proactive Hub, la piattaforma cloud per la Digital Employee Experience (DEX) e la gestione proattiva degli endpoint, fornisce **baramundi Proactive Connect**, un'API per dati di telemetria, metriche DEX e stato degli endpoint. Queste API complementari rendono l'intera infrastruttura baramundi accessibile ai sistemi esterni, consentendo una gamma completa di funzionalità di gestione IT e automazioni.

baramundi Proactive Hub: intelligente, automatizzato e scalabile

baramundi Proactive Hub è una piattaforma intelligente basata su cloud che raccoglie e analizza i dati relativi alle prestazioni e alla sicurezza di DEX su tutti gli endpoint gestiti. Fornisce consigli contestualizzati e consente un intervento correttivo immediato e mirato, offrendo ai team IT una maggiore trasparenza e la capacità di identificare e risolvere i problemi in modo efficace.

2 Cos'è baramundi Proactive Connect?

baramundi Proactive Connect è un'API basata su GraphQL che fornisce accesso programmatico ai dati provenienti da baramundi Proactive Hub. Funge da livello di integrazione tra baramundi Proactive Hub e lo stack tecnologico di gestione IT più ampio, rendendo disponibili le informazioni sugli endpoint dove sono necessarie, anziché tenerle confinate all'interno di strumenti separati.

Gli amministratori IT, gli integratori di sistemi e gli sviluppatori possono utilizzarla per interrogare le informazioni sugli endpoint, integrarle nei flussi di lavoro ed elaborarle automaticamente, direttamente da qualsiasi applicazione di terze parti o dal proprio script.

Panoramica delle caratteristiche principali:

Funzionalità	Descrizione
Tecnologia	GraphQL su HTTPS
Autenticazione	OAuth 2.0 Credenziali client (machine-to-machine)
Formato dati	JSON
Disponibilità	Basato su cloud, Regione UE (connect-euw.baramundi.cloud), Regione USA Est (connect-use.baramundi.cloud)

L'API è progettata per la comunicazione da servizio a servizio: sistemi automatizzati, script e piattaforme di integrazione effettuano l'autenticazione con le proprie credenziali, senza necessità di un login interattivo. Ciò rende baramundi Proactive Connect adatto per attività di automazione pianificate, integrazioni ITSM o dashboard di gestione personalizzate.

Le credenziali vengono assegnate per ogni integrazione e gestite tramite l'interfaccia di amministrazione. Ogni sistema riceve le proprie credenziali con autorizzazioni chiaramente definite. Ciò garantisce un controllo granulare degli accessi e consente la disattivazione di singole integrazioni senza influire sulle altre.

3 Come funziona l'API? – Spiegazione di GraphQL

baramundi Proactive Connect utilizza GraphQL invece della tradizionale architettura REST. La differenza fondamentale è che è la query a determinare quali dati vengono restituiti, non l'API stessa.

3.1 Un unico endpoint per tutto

Tutte le richieste vengono inviate a un unico URL in base alla regione selezionata:

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

Che si tratti di elenchi di endpoint, dati di telemetria o metriche DEX, tutto viene recuperato tramite un unico endpoint utilizzando una richiesta POST. Non ci sono più URL da gestire, né percorsi di risorse con versioni diverse, né formati di risposta incoerenti.

3.2 Solo i dati necessari

La query specifica esattamente quali campi restituire per ridurre il volume dei dati e velocizzare l'elaborazione:

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

Le integrazioni richiedono solo ciò che elaborano: nessun **recupero eccessivo o insufficiente**. Ciò mantiene le query snelle e resilienti ai cambiamenti nel modello di dati.

3.3 ID oggetto univoci

Ogni oggetto nell'API (endpoint, ambiente e applicazione) ha un ID nodo univoco a livello globale. Questi identificatori stabili consentono di fare riferimento in modo affidabile ai record di dati in più query senza confusione causata da nomi duplicati o ID interni mutevoli. Gli ID nodo devono essere utilizzati come stringhe opache: prelevateli direttamente dalle risposte API; non decodificateli né costruiteli autonomamente.

3.4 Esplorazione dello schema e strumenti

Lo schema completo dell'API (tutti i campi, i tipi e le opzioni di query disponibili) può essere recuperato direttamente. L'URL varia a seconda della regione:

```
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}
```

Strumenti come Bruno (open source, desktop), Postman o GraphiQL (basato su browser) caricano questo schema e forniscono il completamento automatico e le descrizioni dei campi integrate mentre si scrivono le query. Se non hai esperienza precedente con GraphQL, questo è il modo più veloce per iniziare: lo schema rende l'intera API esplorabile senza documentazione esterna.

4 Casi d'uso tipici per gli amministratori IT

4.1 Reportistica automatizzata sulla conformità

Scenario: i report mensili di conformità richiedono esportazioni manuali dei dati e un'elaborazione che richiede tempo in strumenti separati. Il processo è soggetto ad errori e spesso impegna le risorse.

Soluzione: uno script PowerShell interroga quotidianamente lo stato di aggiornamento corrente e le metriche DEX per tutti gli endpoint e scrive i risultati direttamente nel sistema ITSM o in una dashboard di reporting. Il report viene generato automaticamente e riflette sempre lo stato attuale. Le deviazioni dallo stato target sono visibili immediatamente, non solo durante la successiva esportazione manuale.

4.2 Dashboard e visualizzazioni

Scenario: i responsabili IT che consolidano l'intera infrastruttura in dashboard di gestione centralizzate possono integrare direttamente le metriche DEX e lo stato degli endpoint dal baramundi Proactive Hub.

Soluzione: i dati degli endpoint e le metriche DEX vengono inviati direttamente alle piattaforme di visualizzazione tramite l'API. Il team IT ha a disposizione tutti i KPI rilevanti a colpo d'occhio nell'interfaccia familiare, consolidati con i dati provenienti da altri sistemi, senza esportazioni manuali o copie di dati.

4.3 Processi automatizzati di onboarding e offboarding

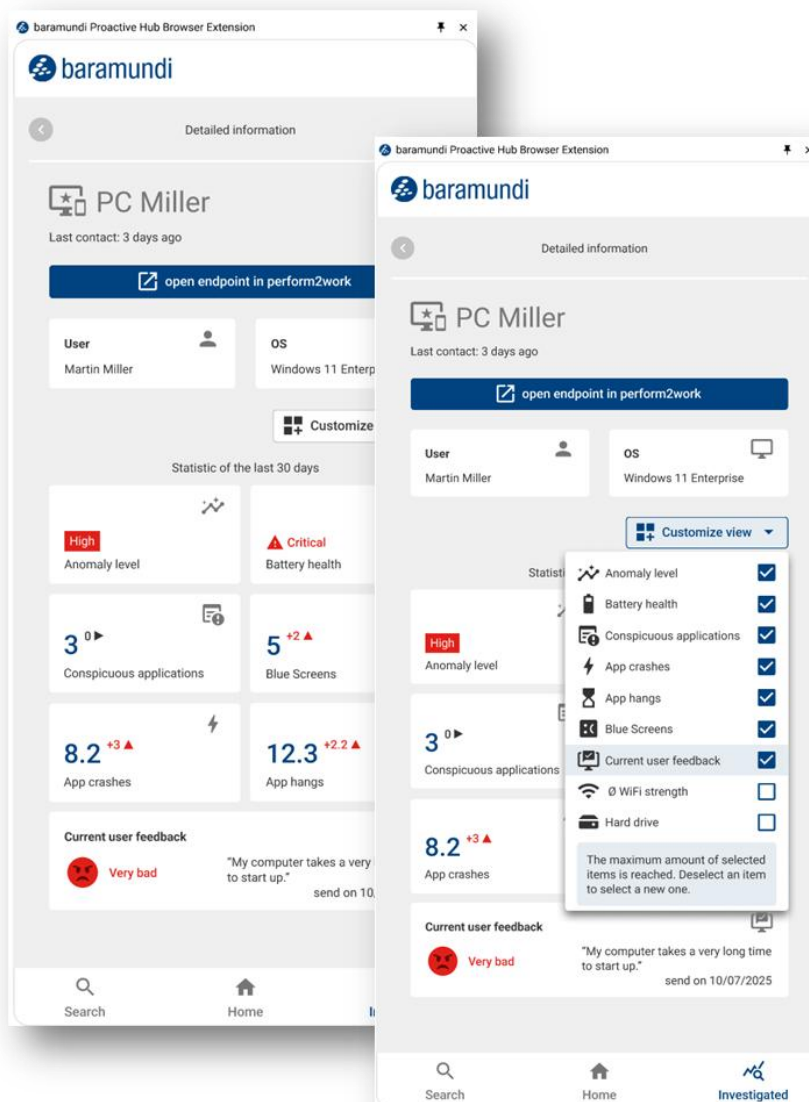
Scenario: quando i dipendenti cambiano ruolo, lo stato e la configurazione dei dispositivi devono essere verificati manualmente e inseriti in più sistemi. Si verificano errori quando le fasi del processo vengono trascurate o eseguite in ritardo.

Soluzione: i flussi di lavoro automatizzati recuperano i dati attuali degli endpoint da baramundi Proactive Hub e attivano le azioni di follow-up necessarie su tutti i sistemi. L'intero processo è verificabile: ogni azione si basa su una chiamata API definita con un risultato registrabile.

4.4 Telemetria degli endpoint direttamente nello strumento ITSM – baramundi Proactive Connect Wave

Scenario: un agente dell'assistenza apre un ticket. Lo strumento ITSM mostra ciò che l'utente ha segnalato, ma non ciò che sta realmente accadendo sull'endpoint interessato. I crash delle app, i problemi di rete o lo stato critico di salute del disco vengono registrati in un sistema separato. Il cambio di contesto richiede tempo e rallenta la risoluzione del problema.

Soluzione: l'estensione per browser **baramundi Proactive Connect Wave** integra i dati in tempo reale degli endpoint provenienti da baramundi Proactive Hub direttamente nello strumento web-based ITSM, CMDB o di gestione delle risorse, senza richiedere alcuna personalizzazione dello strumento o un secondo schermo.



Non appena viene aperto un ticket o si accede ad un endpoint, le informazioni rilevanti appaiono nella barra laterale:

- Blocchi e arresti anomali dell'app
- Qualità della connessione di rete
- Stato del disco
- Feedback degli utenti
- Indicatori delle prestazioni del sistema

Il personale di assistenza può valutare una situazione a colpo d'occhio, stabilire le priorità in modo più efficace e spesso risolvere i problemi prima che l'utente debba richiedere un follow-up.

baramundi Proactive Connect Wave dimostra ciò che un'API aperta consente nella pratica: strumenti third-party e soluzioni interne possono integrare direttamente i dati degli endpoint, senza silos di dati o passaggi manuali.

5 Autenticazione e query iniziale

5.1 Configurazione delle credenziali di accesso

L'accesso a baramundi Proactive Connect richiede credenziali client (Client ID e Client Secret), fornite tramite l'interfaccia di amministrazione. La responsabilità ricade sul rispettivo amministratore baramundi. Istruzioni dettagliate per la configurazione sono disponibili nella documentazione baramundi.

Si consiglia di creare credenziali separate per ogni integrazione per un semplice motivo: ciò consente di disattivare selettivamente singole integrazioni senza influire sulle altre.

5.2 Richiesta di un token di accesso

L'autenticazione utilizza il flusso delle credenziali client OAuth 2.0. L'endpoint di autenticazione è lo stesso per tutte le regioni. Il seguente esempio PowerShell illustra il processo:

```
$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
```

Nota: i segreti client non devono mai essere memorizzati in file di script o repository. Per l'uso in produzione, si consiglia di memorizzarli in un archivio sicuro (ad esempio, PowerShell Secret Management o Azure Key Vault).

5.3 Invia la prima query GraphQL

Con il token ricevuto, è possibile inviare immediatamente la prima query, ad esempio un elenco di tutti gli ambienti disponibili:

```
$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
```

Gli ID dell'ambiente restituiti fungono da punto di partenza per tutte le ulteriori query, come il recupero degli endpoint all'interno di un ambiente specifico.

5.4 Esplorazione dello schema

Per l'uso in produzione, consigliamo uno strumento GraphQL come Bruno (open-source, desktop), Postman o GraphiQL (basato su browser). Tutti e tre caricano lo schema direttamente dall'API e forniscono il completamento automatico e le descrizioni dei campi integrate: un vantaggio significativo rispetto alla creazione manuale delle query.

6 Sicurezza e best practice

Chiunque implementi un'integrazione API è responsabile di garantire la gestione sicura delle credenziali di accesso e dei modelli di query. Le seguenti raccomandazioni si applicano indipendentemente dallo scenario scelto.

6.1 Proteggere le credenziali di accesso

- Non memorizzare mai i segreti dei clienti in file di script, repository o output di log
- Metti i segreti in un archivio dedicato (ad esempio, PowerShell Secret Management o Azure Key Vault)
- Eseguire regolarmente la rotazione delle credenziali di accesso e disattivarle immediatamente se si sospetta una compromissione
- Utilizzare credenziali separate per ogni integrazione: non utilizzare mai un unico segreto condiviso per più sistemi

6.2 Gestione dei token

- I token di accesso scadono dopo un periodo di tempo limitato (il campo ``expires_in`` nella risposta del token specifica il periodo di validità in secondi)
- Rinnova i token in modo proattivo prima che scadano: non aspettare un errore 401 Unauthorized
- Non memorizzare i token in modo permanente; conservali in memoria e richiedine di nuovi quando necessario

6.3 Ottimizzare le query

- Interroga solo i campi necessari: GraphQL consente un controllo preciso su ciò che viene restituito
- Utilizza l'impaginazione per i set di dati di grandi dimensioni: nodi per elenchi semplici e bordi con un cursore per l'impaginazione specifica per posizione
- Trattare gli ID dei nodi come stringhe opache: non decodificarli né costruirli

6.4 Limita l'accesso

- Crea account di servizio separati per diversi scenari di integrazione
- Limita i diritti di accesso al minimo necessario e rivedili regolarmente

7 Conclusione

I sistemi che non comunicano tra loro raddoppiano lo sforzo. I dati degli endpoint visibili solo nel sistema di gestione non sono di alcuna utilità per il personale di supporto nel sistema di ticketing. I dati di telemetria che non confluiscono nei flussi di lavoro non attivano alcuna azione.

baramundi Proactive Connect rende i dati di baramundi Proactive Hub accessibili ai sistemi esterni. I dati di telemetria, le metriche DEX e lo stato degli endpoint sono disponibili tramite l'API GraphQL, sia per script personalizzati, applicazioni di terze parti e soluzioni specializzate come baramundi Proactive Connect Wave.

Insieme a baramundi Connect per la baramundi Management Suite, ciò fornisce una base API completa: due interfacce che si completano a vicenda e aprono l'intera infrastruttura baramundi ai sistemi esterni.

Per i team IT, ciò significa:

- Meno lavoro manuale grazie a flussi di lavoro basati su API
- Tempi di risposta più brevi grazie all'analisi diretta dei dati di telemetria
- Migliore processo decisionale grazie all'integrazione in dashboard e sistemi ITSM esistenti
- Un'architettura pronta per il futuro, costruita con tecnologie aperte e standardizzate (GraphQL / OAuth 2.0)
- Scalabile: ogni nuova integrazione si basa sulla stessa base condivisa

Ulteriori informazioni, documentazione e script di esempio:

github.com/baramundisoftware/Proactive-Connect

I team IT che stanno valutando baramundi Proactive Hub possono richiedere la nostra versione completa gratuita per 30 giorni o un'implementazione proof-of-concept sulla propria rete per verificare di persona i vantaggi.

Prova subito la versione completa: [baramundi Proactive Hub](#)

Contattaci!

Non vediamo l'ora di conoscerti!



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