



Control API - Technical Interface Guide

API Reference, Reporting Interfaces, Monitor/Beam Operations and Service Evidence

Technische Referenz für NOC, Integratoren und Betriebsautomatisierung

Code-inventarisierte FastAPI-Routen: 265

Planned / Proposed Routen: 20

Produktkontext: Control für Umgebungen mit Extreme Networks XIQ, WiNG und ExtremeControl / Site Engine. Kein offizielles Extreme-Networks-Produkt.

Inhaltsverzeichnis

- 1 Executive Technical Overview
- 2 Base URLs
- 3 Authentifizierung
- 4 Version, Health und Build
- 5 Monitor / Insight
- 6 Workspace
- 7 AP Investigation
- 8 Client Investigation
- 9 Service Diagnostics
- 10 Reporting API
- 11 Planned Reporting API
- 12 Evidence / PCAP
- 13 Beam API
- 14 Beam Companion / Mobile API
- 15 Operations / Update / Backup / Restore
- 16 Control Internal Services API
- 17 Response Standards
- 18 Error Handling
- 19 Security / Datenschutz
- 20 Curl-Sammlung
- 21 Appendix und Endpoint-Inventar

1. Executive Technical Overview

Control bietet technische Schnittstellen für Monitoring, Diagnose, Reporting, Evidence, Beam und Operations. Typische Integrationen sind NOC-Dashboards, Ticketing, externe Automatisierung, Reporting, eigene Betriebsüberwachung und Remote-Site-Steuerung.

Die Inventarisierung unterscheidet Public, Auth, Admin und Agent/Token. Die finale Autorisierung bleibt eine serverseitige Entscheidung; diese Referenz leitet sie aus sichtbaren Code-Guards ab.

2. Base URLs

Control API: <https://api.company.com>. Update Feed: <https://updates.company.com>. Lokales Installationsbeispiel: <http://<control-host>:8000>.

Die lokale Adresse ist ein Platzhalter. Produktive Integrationen verwenden den freigegebenen API-Host oder eine dokumentierte interne Adresse.

3. Authentifizierung

Public-Routen verwenden typischerweise `/api/public/`. Auth-Routen benötigen Bearer-Token oder Control-Sitzung, Admin-Routen zusätzlich Administratorrechte. Agent/Token-Routen sind für Beam- oder Companion-Enrollments vorgesehen.

Tokens niemals in URLs, Tickets, Screenshots, PDFs oder Browser-Logs ablegen.

```
BASE='https://api.company.com'  
TOKEN='YOUR_CONTROL_TOKEN'  
curl -s -H "Authorization: Bearer $TOKEN" "$BASE/api/version"
```

4. Version, Health und Build API

Available: Version, Health, System Status, öffentliche Settings und geschützte Dokumentationsrouten. Der Admin-OpenAPI-Export `/api/docs/openapi.json` wurde im Code erkannt, aber ohne Credentials nicht live abgerufen.

Methode	Endpoint	Zugriff	Zweck
GET	/api/docs/inventory	Admin	get protected api inventory
GET	/api/docs/openapi.json	Admin	get protected openapi
GET	/api/health	Route guard prüfen	Runtime- und Dependency-Health
GET	/api/settings/public	Route guard prüfen	Control Settings, Storage oder Logs
GET	/api/system/status	Auth	get system status
GET	/api/version	Route guard prüfen	Build-, Version- und Git-Metadaten

5. Monitor / Insight API

Monitor liefert gespeicherte, sanitierte Snapshots, Datenbankstatus, Collector-, Ingestion- und Schedulerstatus sowie Workspace-Scopes. Public-Antworten enthalten keine sensiblen Client-Identitäten.

Wichtige verfügbare Pfade sind /api/public/monitor/db/status, /api/monitor/db/status, /api/monitor/db/initialize, /api/monitor/live-snapshot/save, /api/public/monitor/collector/status, /api/monitor/collector/collect-now und die Workspace-Routen.

Methode	Endpoint	Zugriff	Zweck
POST	/api/monitor/collector/collect-now	Admin	Manueller, begrenzter Collector-Lauf
GET	/api/monitor/collector/status	Auth	Collector-Status und effektive Intervalle
POST	/api/monitor/db/initialize	Admin	control monitor db initialize
GET	/api/monitor/db/status	Auth	Monitor-Datenbank- und Storage-Status
GET	/api/monitor/foundation	Auth	get monitor foundation status
GET	/api/monitor/ingestion/status	Auth	control monitor ingestion status
POST	/api/monitor/ingestion/xiq-snapshot/preview	Admin	control monitor xiq snapshot preview
POST	/api/monitor/ingestion/xiq-snapshot/run	Admin	control monitor xiq snapshot run
GET	/api/monitor/live-snapshot/preview	Auth	control monitor live snapshot preview
POST	/api/monitor/live-snapshot/save	Admin	control monitor live snapshot save
POST	/api/monitor/maintenance/confirm-action	Admin	control monitor maintenance confirm action
POST	/api/monitor/maintenance/reset-data	Admin	control monitor maintenance reset data
POST	/api/monitor/maintenance/settings	Admin	Control Settings, Storage oder Logs
GET	/api/monitor/maintenance/status	Auth	control monitor maintenance status
GET	/api/monitor/overview	Route guard prüfen	control monitor overview
GET	/api/monitor/query-contracts	Auth	control monitor query contracts
GET	/api/monitor/read-model	Route guard prüfen	control monitor read model
POST	/api/monitor/scheduler/preview	Admin	control monitor scheduler preview
POST	/api/monitor/scheduler/run-due	Admin	control monitor scheduler run due
GET	/api/monitor/scheduler/status	Auth	control monitor scheduler status
GET	/api/monitor/snapshot-trends	Auth	control monitor snapshot trends
POST	/api/monitor/usage-collect	Admin	control monitor usage collect
GET	/api/monitor/usage-scout	Admin	control monitor usage scout
GET	/api/monitor/workspace	Auth	Scope-basierter Monitor Workspace und Investigation
GET	/api/monitor/xiq-data-source-map	Auth	control monitor xiq data source map
GET	/api/public/monitor/collector/status	Public	Collector-Status und effektive Intervalle
GET	/api/public/monitor/db/status	Public	Monitor-Datenbank- und Storage-Status
GET	/api/public/monitor/foundation	Public	get public monitor foundation status
GET	/api/public/monitor/ingestion/status	Public	control public monitor ingestion status
GET	/api/public/monitor/live-snapshot/status	Public	control public monitor live snapshot status
GET	/api/public/monitor/maintenance/status	Public	control public monitor maintenance status
GET	/api/public/monitor/overview	Public	control public monitor overview

Methode	Endpoint	Zugriff	Zweck
GET	/api/public/monitor/query-contracts	Public	control public monitor query contracts
GET	/api/public/monitor/read-model	Public	control public monitor read model
GET	/api/public/monitor/scheduler/status	Public	control public monitor scheduler status
GET	/api/public/monitor/snapshot-trends	Public	control public monitor snapshot trends
GET	/api/public/monitor/workspace	Public	Scope-basierter Monitor Workspace und Investigation
GET	/api/public/monitor/xiq-data-source-map	Public	control public monitor xiq data source map
GET	/api/public/monitor/xiq-source-catalog	Public	control public monitor xiq source catalog

6. Workspace API

Query-Parameter: window_hours, time_from, time_to, metric, bucket_minutes, site, building, floor, ssid, vlan, ap, client, q, view, limit und facet_limit. Metriken umfassen clients und throughput. RX/TX stammen aus echten Counter-Deltas; SSID/VLAN/Client-Throughput wird nicht aus AP-Interface-Zählern erfunden.

```
curl -sG "$BASE/api/monitor/workspace" \
-H "Authorization: Bearer $TOKEN" \
--data-urlencode "ap=AP-Lobby-01" \
--data-urlencode "window_hours=24" \
--data-urlencode "metric=throughput"
```

7. AP Investigation API

AP Investigation wird über den authentifizierten Workspace mit ap=<Demo-AP> aufgebaut. Radio-Switcher, per-Radio-Throughput, gespeicherte Clients und Availability sind nur so vollständig wie die persistierten Monitor-Samples.

Nicht Available: /api/monitor/ap-live-snapshot sowie ein AP-Live-SSH-Refresh wurden im aktuellen Code-Inventar nicht gefunden. Der unten aufgeführte Entwurf ist Roadmap, nicht nutzbar.

```
# Proposed, nicht ausführen als verfügbare API
curl -s -X POST "$BASE/api/monitor/ap-live-snapshot" \
-H "Authorization: Bearer $TOKEN" \
-H 'Content-Type: application/json' \
-d '{"ap": "AP-Lobby-01", "force_refresh": true}'
```

8. Client Investigation API

client_detail liefert identity, context, current, timelines, summaries und availability. Client Usage, RSSI, SNR, Noise, Band/Kanal, direkte bps und Roaming erscheinen ausschließlich, wenn persistierte client_session-Snapshots sie enthalten. AP-Kontext ist eine getrennte sekundäre Serie.

```
curl -sG "$BASE/api/monitor/workspace" \
-H "Authorization: Bearer $TOKEN" \
--data-urlencode "client=demo-macbook" \
--data-urlencode "window_hours=24" \
| jq '.client_detail | {identity, context, current, availability}'
```

9. Service Diagnostics API

Available Routen decken Management Tests, DNS-Evidence-Sweeps, XIQ AP Actions und NAC-Tests ab. DHCP, Gateway, NTP, RADIUS und Cloud Services sind nur dann als dedizierter Contract verfügbar, wenn sie im Inventar stehen; sonst sind sie Planned / Proposed.

Methode	Endpoint	Zugriff	Zweck
GET	/api/integrations/servicenow/foundation	Auth	get servicenow foundation status
POST	/api/nac/clearpass/test	Route guard prüfen	test nac clearpass connection
GET	/api/nac/site-engine/summary	Route guard prüfen	get nac site engine summary
POST	/api/nac/site-engine/test	Route guard prüfen	test nac site engine connection
GET	/api/public/integrations/servicenow/foundation	Public	get public servicenow foundation status
GET	/api/public/integrations/servicenow/outbox-preview	Public	control public servicenow outbox preview

Methode	Endpoint	Zugriff	Zweck
GET	/api/xiq/access-points	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/access-points/{ap_id}/refresh-now	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/accounts	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/accounts/switch	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/acsp-cli-neighbors	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/cli	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/clients/refresh	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/disconnect-clients	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/management-test	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/packet-capture/start	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
DELETE	/api/xiq/ap-actions/{device_id}/packet-capture/{job_id}	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/ap-actions/{device_id}/packet-capture/{job_id}	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/packet-capture/{job_id}/archive	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/ap-actions/{device_id}/packet-capture/{job_id}/download	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/packet-capture/{job_id}/stop	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/ping	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/ping-device	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/radio-interfaces	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/reboot	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/traceroute	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/vlan-probe	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/vlan-probe-cli	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/ap-neighbors/{device_id}	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/cache/clear-runtime-and-refresh	Admin	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/cache/refresh	Admin	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/cache/refresh-metadata	Admin	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/cache/status	Auth	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/client-details/{client_id}	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/client-experience/{client_id}	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/client-roaming/{client_id}	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/client-troubleshoot	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/clients/active	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/clients/active/count	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/clients/active/counts	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/clients/live-refresh	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/debug/config	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/devices	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/locations	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/login	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/nac/scope-test	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/pcap/download-url	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/portal-status	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/token-info	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose

Methode	Endpoint	Zugriff	Zweck
GET	/api/xiq/wlan-config	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose

10. Reporting API

Available: Report Engine Status, Templates, Jobs, Preview und Job-Erstellung. Full Report, Issue Report, HTML/PDF-Ausgabe, Executive Summary, Tested Services Summary, Root Cause Correlation, Affected Infrastructure, Timeline und Evidence werden über Templates und Gates verifiziert.

Identity Modes sind fachlich full, anonymized und management_summary. Der konkrete Template-Contract ist über /api/report-engine/jobs/templates zu lesen.

Methode	Endpoint	Zugriff	Zweck
GET	/api/public/report-engine/foundation	Public	Report Engine Status, Templates oder Jobs
GET	/api/public/report-engine/jobs/status	Public	Report Engine Status, Templates oder Jobs
GET	/api/public/report-engine/jobs/templates	Public	Report Engine Status, Templates oder Jobs
GET	/api/report-engine/foundation	Auth	Report Engine Status, Templates oder Jobs
GET	/api/report-engine/jobs	Route guard prüfen	Report Engine Status, Templates oder Jobs
POST	/api/report-engine/jobs	Route guard prüfen	Report Engine Status, Templates oder Jobs
POST	/api/report-engine/jobs/preview	Route guard prüfen	Report Engine Status, Templates oder Jobs
GET	/api/report-engine/jobs/status	Route guard prüfen	Report Engine Status, Templates oder Jobs

11. Geplante Reporting-Endpunkte - Planned / Proposed

Nicht als aktuelle FastAPI-Routen gefunden: DNS (Resolver/Lookup Evidence), DHCP (Reply/VLAN Impact), NTP (Reachability/Drift), Gateway (Ping/Loss/VLAN Impact), RADIUS (Auth/Accounting Evidence), NAC (Policy/Onboarding) und Cloud Services (CAPWAP/Telemetry/Keepalive).

Gemeinsame Parameter: site, building, ap, client, ssid, vlan, time_from, time_to, severity, identity_mode und optional format=json|html|pdf. Vorgesehene Response: ok, status, generated_at, scope, severity, summary und evidence.

Methode	Endpoint	Zugriff	Zweck
GET	/api/reports/dns	Planned	proposed dns report
POST	/api/reports/dns/run	Planned	proposed dns run
GET	/api/reports/dhcp	Planned	proposed dhcp report
POST	/api/reports/dhcp/run	Planned	proposed dhcp run
GET	/api/reports/ntp	Planned	proposed ntp report
POST	/api/reports/ntp/run	Planned	proposed ntp run
GET	/api/reports/gateway	Planned	proposed gateway report
POST	/api/reports/gateway/run	Planned	proposed gateway run
GET	/api/reports/radius	Planned	proposed radius report
POST	/api/reports/radius/run	Planned	proposed radius run
GET	/api/reports/nac	Planned	proposed nac report
POST	/api/reports/nac/run	Planned	proposed nac run
GET	/api/reports/cloud-services	Planned	proposed cloud-services report
POST	/api/reports/cloud-services/run	Planned	proposed cloud-services run

12. Evidence / PCAP API

Capture-Jobs, Remote Sniffer und Techdumps sind Evidence-Operationen. Vor Ausführung Scope, Filter/BPF, Frame Limit, Duration, Job-Status, sicheren Stop und Cleanup prüfen. PCAP- und Techdump-Daten sind sensitiv.

```
curl -s -X POST "$BASE/api/captures/route-preview" \
-H "Authorization: Bearer $TOKEN" \
-H 'Content-Type: application/json' \
```

```
-d '{"ap_id":"demo-ap-id","duration_seconds":60,"frame_limit":5000}'
```

Methode	Endpoint	Zugriff	Zweck
GET	/api/captures	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/captures/bulk-download	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/captures/route-preview	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/captures/start	Route guard prüfen	Evidence Capture / PCAP-Steuerung
DELETE	/api/captures/{job_id}	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/captures/{job_id}	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/captures/{job_id}/analysis	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/captures/{job_id}/download	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/captures/{job_id}/hard-stop	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/captures/{job_id}/retry-export	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/captures/{job_id}/status	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/captures/{job_id}/stop	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/client-troubleshoot/remote-sniffer/jobs	Route guard prüfen	Evidence Capture / PCAP-Steuerung
DELETE	/api/client-troubleshoot/remote-sniffer/jobs/{job_id}	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/client-troubleshoot/remote-sniffer/jobs/{job_id}	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/client-troubleshoot/remote-sniffer/jobs/{job_id}/download	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/client-troubleshoot/remote-sniffer/jobs/{job_id}/stop	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/client-troubleshoot/remote-sniffer/start	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/techdumps	Route guard prüfen	Techdump-Job und Download
POST	/api/techdumps/route-preview	Route guard prüfen	Techdump-Job und Download
POST	/api/techdumps/start	Route guard prüfen	Techdump-Job und Download
DELETE	/api/techdumps/{techdump_id}	Route guard prüfen	Techdump-Job und Download
GET	/api/techdumps/{techdump_id}/download	Route guard prüfen	Techdump-Job und Download
POST	/api/techdumps/{techdump_id}/stop	Route guard prüfen	Techdump-Job und Download

13. Beam API

Beam bedient Remote Sites über Enrollment, Heartbeat und Job Claim/Progress/Result. Der Agent kann begrenzte, erlaubte Management-Tests ausführen. Der Ablauf folgt Server-, Token-, Enrollment- und Scope-Guards.

Methode	Endpoint	Zugriff	Zweck
GET	/api/beam-updates/foundation	Auth	get beam update foundation status
POST	/api/beam/captures/{job_id}/upload	Agent/Token	Evidence Capture / PCAP-Steuerung
POST	/api/beam/enroll	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
GET	/api/beam/firmware/files/{version}/{family_key}/{filename}	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beam/heartbeat	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beam/jobs/claim	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beam/jobs/control	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beam/jobs/progress	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beam/jobs/result	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beam/techdumps/{techdump_id}/upload	Agent/Token	Techdump-Job und Download
GET	/api/beams	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beams	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
DELETE	/api/beams/{beam_id}	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
GET	/api/beams/{beam_id}	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung

Methode	Endpoint	Zugriff	Zweck
PATCH	/api/beams/{beam_id}	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
PATCH	/api/beams/{beam_id}/assignments	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beams/{beam_id}/assignments	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
DELETE	/api/beams/{beam_id}/assignments/{assignment_id}	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
PATCH	/api/beams/{beam_id}/capabilities	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beams/{beam_id}/disable	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beams/{beam_id}/enable	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
GET	/api/beams/{beam_id}/jobs	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beams/{beam_id}/jobs	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
GET	/api/beams/{beam_id}/jobs/{job_id}	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beams/{beam_id}/rotate-token	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/companion/enroll	Agent/Token	enroll companion
POST	/api/companion/heartbeat	Agent/Token	companion heartbeat
GET	/api/companions	Route guard prüfen	list companions
POST	/api/companions	Route guard prüfen	create companion
DELETE	/api/companions/{companion_id}	Route guard prüfen	delete companion
GET	/api/companions/{companion_id}	Route guard prüfen	get companion
POST	/api/companions/{companion_id}/disable	Route guard prüfen	disable companion
POST	/api/companions/{companion_id}/enable	Route guard prüfen	enable companion
POST	/api/companions/{companion_id}/rotate-token	Route guard prüfen	rotate companion token
GET	/api/public/beam-updates/foundation	Public	get public beam update foundation status

14. Beam Companion / Mobile API

Companion/Mobile bietet Enrollment, Heartbeat, Mobile Summary, AP-/Client-Listen und begrenzte mobile Tests. QR- und Manual-Enrollment sind ausschließlich über die tatsächlich vorhandenen Enrollment-Routen verfügbar.

Methode	Endpoint	Zugriff	Zweck
GET	/api/mobile/access-points	Route guard prüfen	mobile access points
POST	/api/mobile/access-points/{access_point_id}/client-vlan-tests	Route guard prüfen	mobile access point client vlan test
POST	/api/mobile/access-points/{access_point_id}/dhcp-test	Route guard prüfen	mobile access point dhcp test
POST	/api/mobile/access-points/{access_point_id}/tests/{test_name}	Route guard prüfen	mobile access point test
GET	/api/mobile/clients	Route guard prüfen	mobile clients
POST	/api/mobile/clients/{client_id}/troubleshoot	Route guard prüfen	mobile client troubleshoot
GET	/api/mobile/summary	Route guard prüfen	mobile summary

15. Operations / Update / Backup / Restore API

Available: Settings, Storage, Backups, Restore, Setup, Update-Status, Update-Plan, Update-Jobs und Execution-nahe Operationen. Für automatisierte Writes sind Rolle, Wartungsfenster, Preview/Dry-Run, Bestätigung und Recovery-Plan erforderlich.

Methode	Endpoint	Zugriff	Zweck
GET	/api/public/system/env-doctor	Public	control public env doctor
GET	/api/public/system/feature-gates	Public	get public system feature gates
GET	/api/settings	Auth	Control Settings, Storage oder Logs
PUT	/api/settings	Admin	Control Settings, Storage oder Logs

Methode	Endpoint	Zugriff	Zweck
GET	/api/settings/logs/download	Auth	Control Settings, Storage oder Logs
GET	/api/settings/public	Route guard prüfen	Control Settings, Storage oder Logs
GET	/api/settings/storage	Auth	Control Settings, Storage oder Logs
POST	/api/system/backup-schedules/{job_id}/run-now	Auth	run scheduled backup now
GET	/api/system/backups	Auth	Backup / Restore Operations
POST	/api/system/backups/create	Auth	Backup / Restore Operations
DELETE	/api/system/backups/{backup_id}	Auth	Backup / Restore Operations
POST	/api/system/backups/{backup_id}/cancel	Auth	Backup / Restore Operations
PATCH	/api/system/backups/{backup_id}/comment	Auth	Backup / Restore Operations
GET	/api/system/backups/{backup_id}/download	Auth	Backup / Restore Operations
GET	/api/system/env-doctor	Auth	control env doctor
GET	/api/system/feature-gates	Auth	get system feature gates
GET	/api/system/migration-data-dry-run	Auth	get system migration data dry run
POST	/api/system/migration-execute	Admin	post system migration execute
GET	/api/system/migration-execution-dry-run	Admin	get system migration execution dry run
GET	/api/system/migration-full-dry-run-plan	Auth	get system migration full dry run plan
GET	/api/system/migration-postgres-compare	Auth	get system migration postgres compare
GET	/api/system/migration-readiness	Auth	get system migration readiness
GET	/api/system/migration-schema-dry-run	Auth	get system migration schema dry run
GET	/api/system/migration-target-validation	Auth	get system migration target validation
POST	/api/system/monitor-db/check	Auth	check system monitor database
POST	/api/system/monitor-db/initialize	Admin	initialize system monitor database
POST	/api/system/restore/execute	Admin	Backup / Restore Operations
GET	/api/system/restore/maintenance	Admin	Backup / Restore Operations
PUT	/api/system/restore/maintenance	Admin	Backup / Restore Operations
POST	/api/system/restore/prepare-candidate	Admin	Backup / Restore Operations
POST	/api/system/restore/prepare-existing	Admin	Backup / Restore Operations
GET	/api/system/restore/sessions/{restore_session_id}	Admin	Backup / Restore Operations
POST	/api/system/restore/sessions/{restore_session_id}/safely-backup	Admin	Backup / Restore Operations
POST	/api/system/restore/validate-upload	Auth	Backup / Restore Operations
POST	/api/system/setup/complete	Admin	post system setup complete
POST	/api/system/setup/reset	Admin	post system setup reset
GET	/api/system/setup/status	Auth	get system setup status
POST	/api/system/setup/test-nac	Admin	post system setup test nac
POST	/api/system/setup/test-xiq	Admin	post system setup test xiq
POST	/api/system/setup/validate	Admin	post system setup validate
GET	/api/system/status	Auth	get system status
GET	/api/system/update-audit	Auth	Update Planning, Jobs und Execution
POST	/api/system/update-check	Auth	Update Planning, Jobs und Execution
POST	/api/system/update-execute	Admin	Update Planning, Jobs und Execution
GET	/api/system/update-execution/components	Route guard prüfen	Update Planning, Jobs und Execution
POST	/api/system/update-execution/execute	Route guard prüfen	Update Planning, Jobs und Execution
GET	/api/system/update-execution/jobs/{job_id}	Route guard prüfen	Update Planning, Jobs und Execution
GET	/api/system/update-execution/status	Route guard prüfen	Update Planning, Jobs und Execution
GET	/api/system/update-jobs	Auth	Update Planning, Jobs und Execution
POST	/api/system/update-jobs/dry-run	Admin	Update Planning, Jobs und Execution

Methode	Endpoint	Zugriff	Zweck
GET	/api/system/update-jobs/{job_id}	Auth	Update Planning, Jobs und Execution
POST	/api/system/update-plan	Auth	Update Planning, Jobs und Execution
GET	/api/system/update-status	Auth	Update Planning, Jobs und Execution

16. Control Internal Services API - Planned / Proposed

Heute liefern /api/version, /api/health, System-, Settings- und Update-Routen Teilinformationen. Der folgende Vertragsentwurf ergänzt Service-/Container-Status, service-spezifische Health, begrenzte redigierte Logs und stark geschützte Restarts.

Keine Container-Environments ausgeben, Tokens nie loggen, Logs redigieren und begrenzen. Erwartete Dienste: control-frontend, control-backend-api, control-postgres, control-monitor-timescale, control-updater, control-supervisor, control-recovery-sidecar, beam-agent und control-website.

Methode	Endpoint	Zugriff	Zweck
GET	/api/operations/services	Planned/Admin	proposed services
GET	/api/operations/services/{service}	Planned/Admin	proposed service
GET	/api/operations/services/{service}/health	Planned/Admin	proposed service health
GET	/api/operations/services/{service}/logs?lines=200	Planned/Admin	proposed service logs
POST	/api/operations/services/{service}/restart	Planned/Admin	proposed service restart
GET	/api/operations/containers	Planned/Admin	proposed containers

17. API Response Standards

Erwartbare Response-Felder sind ok, status, message, generated_at, source, cache_state, availability, items, jobs oder templates. Nicht jede historische Route liefert alle Felder. Integratoren müssen unbekannte Felder tolerant behandeln.

Pagination, Time Range und Severity sind route-spezifisch; limit, window_hours, time_from, time_to und severity gegen den konkreten Contract prüfen.

18. Error Handling

400: ungültige Parameter. 401: Token/Sitzung fehlt. 403: Rolle fehlt. 404: Ressource nicht gefunden. 409: Konflikt. 429: Rate Limit - Backoff mit Jitter. 500: interner Fehler. 503: Abhängigkeit wie DB, XIQ, Beam oder Update Service nicht verfügbar. Bei Timeout, Beam offline oder AP SSH unavailable nur korrelationsfähige, nicht-sensitive Diagnosedaten erfassen.

19. Security und Datenschutz

Public API darf keine MAC-, IP- oder Usernamen enthalten. Auth API liefert nur zulässige Labels. Keine Secrets in Responses; Tokens nie in URLs. Logs redigieren und PCAP/Techdump als sensitive Evidence behandeln. Demo-Werte: Demo Campus, AP-Lobby-01, demo-macbook und Client VLAN 192.

20. Copy-Paste Curl-Sammlung

```

BASE='https://api.company.com'
TOKEN='YOUR_CONTROL_TOKEN'

# Version
curl -s "$BASE/api/version" | jq

# Health
curl -s "$BASE/api/health" | jq

# Beta update feed
curl -s 'https://updates.company.com/api/releases/beta' | jq

# Public Monitor DB status
curl -s "$BASE/api/public/monitor/db/status" | jq

```

```
# Auth collector status
curl -s -H "Authorization: Bearer $TOKEN" "$BASE/api/monitor/collector/status" | jq

# Workspace overview
curl -sG -H "Authorization: Bearer $TOKEN" "$BASE/api/monitor/workspace" --data-urlencode 'window_hours=24' | jq

# Proposed DNS report - not Available
curl -sG -H "Authorization: Bearer $TOKEN" "$BASE/api/reports/dns" --data-urlencode 'site=Demo Campus'

# Proposed service status - not Available
curl -s -H "Authorization: Bearer $TOKEN" "$BASE/api/operations/services"
```

21. Appendix: Vollständiges Endpoint-Inventar aus Code

Code-deklarierte Routen, nach funktionalem Bereich gruppiert. Zugriff ist aus sichtbaren Route-Guards abgeleitet und vor produktiver Nutzung gegen den Admin-OpenAPI-Export zu prüfen.

Auth / Admin

Methode	Endpoint	Zugriff	Zweck
GET	/api/admin/api-tokens	Admin	list control api tokens
POST	/api/admin/api-tokens	Admin	create control api token
DELETE	/api/admin/api-tokens/{token_id}	Admin	revoke control api token
GET	/api/admin/identity-foundation	Admin	get identity foundation
DELETE	/api/admin/logging/events	Route guard prüfen	clear control logging events
GET	/api/admin/logging/events	Route guard prüfen	get control logging events
GET	/api/admin/users	Admin	list control users
POST	/api/admin/users	Admin	create control user
PUT	/api/admin/users/{user_id}	Admin	update control user
PUT	/api/admin/users/{user_id}/password	Admin	update control user password
PUT	/api/admin/xiq-service-account	Admin	update xiq service account
GET	/api/admin/xiq-service-account/status	Admin	get xiq service account status
POST	/api/admin/xiq-service-account/test	Admin	test xiq service account
POST	/api/auth/login	Route guard prüfen	login control user
POST	/api/auth/logout	Route guard prüfen	logout control user
GET	/api/auth/me	Route guard prüfen	get control auth me

Beam / Companion

Methode	Endpoint	Zugriff	Zweck
GET	/api/beam-updates/foundation	Auth	get beam update foundation status
POST	/api/beam/captures/{job_id}/upload	Agent/Token	Evidence Capture / PCAP-Steuerung
POST	/api/beam/enroll	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
GET	/api/beam/firmware/files/{version}/{family_key}/{filename}	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beam/heartbeat	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beam/jobs/claim	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beam/jobs/control	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beam/jobs/progress	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beam/jobs/result	Agent/Token	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beam/techdumps/{techdump_id}/upload	Agent/Token	Techdump-Job und Download
GET	/api/beams	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beams	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
DELETE	/api/beams/{beam_id}	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
GET	/api/beams/{beam_id}	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
PATCH	/api/beams/{beam_id}	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
PATCH	/api/beams/{beam_id}/assignments	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beams/{beam_id}/assignments	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
DELETE	/api/beams/{beam_id}/assignments/{assignment_id}	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
PATCH	/api/beams/{beam_id}/capabilities	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung

Methode	Endpoint	Zugriff	Zweck
POST	/api/beams/{beam_id}/disable	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beams/{beam_id}/enable	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
GET	/api/beams/{beam_id}/jobs	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beams/{beam_id}/jobs	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
GET	/api/beams/{beam_id}/jobs/{job_id}	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/beams/{beam_id}/rotate-token	Route guard prüfen	Beam Enrollment, Heartbeat oder Job-Steuerung
POST	/api/companion/enroll	Agent/Token	enroll companion
POST	/api/companion/heartbeat	Agent/Token	companion heartbeat
GET	/api/companions	Route guard prüfen	list companions
POST	/api/companions	Route guard prüfen	create companion
DELETE	/api/companions/{companion_id}	Route guard prüfen	delete companion
GET	/api/companions/{companion_id}	Route guard prüfen	get companion
POST	/api/companions/{companion_id}/disable	Route guard prüfen	disable companion
POST	/api/companions/{companion_id}/enable	Route guard prüfen	enable companion
POST	/api/companions/{companion_id}/rotate-token	Route guard prüfen	rotate companion token
GET	/api/public/beam-updates/foundation	Public	get public beam update foundation status

Core / Other

Methode	Endpoint	Zugriff	Zweck
GET	/api/ap-control-reachability	Route guard prüfen	get ap control reachability
GET	/api/ap-operational-cache	Route guard prüfen	get ap operational cache
POST	/api/ap-operational-cache/poe/refresh-missing	Route guard prüfen	refresh missing poe cache
POST	/api/ap-operational-cache/{device_id}/ensure	Route guard prüfen	ensure ap operational cache for ap
POST	/api/client-vlan/dns-evidence-sweep/start	Route guard prüfen	start client vlan dns evidence sweep
GET	/api/client-vlan/dns-evidence-sweep/{job_id}	Route guard prüfen	get client vlan dns evidence sweep
POST	/api/client-vlan/dns-evidence-sweep/{job_id}/stop	Route guard prüfen	stop client vlan dns evidence sweep
GET	/api/docs/inventory	Admin	get protected api inventory
GET	/api/docs/openapi.json	Admin	get protected openapi
POST	/api/emm/soti/test	Route guard prüfen	test emm soti connection
GET	/api/health	Route guard prüfen	Runtime- und Dependency-Health
GET	/api/jobs	Auth	list jobs
GET	/api/management-test-history	Route guard prüfen	get management test history
GET	/api/ops/foundation	Auth	get ops foundation status
GET	/api/public/ops/foundation	Public	get public ops foundation status
GET	/api/public/ssh-engine/foundation	Public	get public ssh engine foundation status
GET	/api/ssh-engine/foundation	Auth	get ssh engine foundation status
GET	/api/version	Route guard prüfen	Build-, Version- und Git-Metadaten

Evidence / Capture

Methode	Endpoint	Zugriff	Zweck
GET	/api/captures	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/captures/bulk-download	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/captures/route-preview	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/captures/start	Route guard prüfen	Evidence Capture / PCAP-Steuerung
DELETE	/api/captures/{job_id}	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/captures/{job_id}	Route guard prüfen	Evidence Capture / PCAP-Steuerung

Methode	Endpoint	Zugriff	Zweck
GET	/api/captures/{job_id}/analysis	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/captures/{job_id}/download	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/captures/{job_id}/hard-stop	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/captures/{job_id}/retry-export	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/captures/{job_id}/status	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/captures/{job_id}/stop	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/client-troubleshoot/remote-sniffer/jobs	Route guard prüfen	Evidence Capture / PCAP-Steuerung
DELETE	/api/client-troubleshoot/remote-sniffer/jobs/{job_id}	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/client-troubleshoot/remote-sniffer/jobs/{job_id}	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/client-troubleshoot/remote-sniffer/jobs/{job_id}/download	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/client-troubleshoot/remote-sniffer/jobs/{job_id}/stop	Route guard prüfen	Evidence Capture / PCAP-Steuerung
POST	/api/client-troubleshoot/remote-sniffer/start	Route guard prüfen	Evidence Capture / PCAP-Steuerung
GET	/api/techdumps	Route guard prüfen	Techdump-Job und Download
POST	/api/techdumps/route-preview	Route guard prüfen	Techdump-Job und Download
POST	/api/techdumps/start	Route guard prüfen	Techdump-Job und Download
DELETE	/api/techdumps/{techdump_id}	Route guard prüfen	Techdump-Job und Download
GET	/api/techdumps/{techdump_id}/download	Route guard prüfen	Techdump-Job und Download
POST	/api/techdumps/{techdump_id}/stop	Route guard prüfen	Techdump-Job und Download

Jobs / Firmware

Methode	Endpoint	Zugriff	Zweck
POST	/api/firmware/upload	Route guard prüfen	api upload firmware auto
GET	/api/firmware/versions	Route guard prüfen	api list firmware versions
POST	/api/firmware/versions	Route guard prüfen	api create firmware version
DELETE	/api/firmware/versions/{version}	Route guard prüfen	api delete firmware version
DELETE	/api/firmware/versions/{version}/models/{model_key}	Route guard prüfen	api delete firmware model
POST	/api/firmware/versions/{version}/models/{model_key}/upload	Route guard prüfen	api upload firmware model
POST	/api/jobs/firmware-upgrade	Route guard prüfen	create firmware upgrade job
POST	/api/jobs/firmware-upgrade/config-preview	Route guard prüfen	preview firmware upgrade config
POST	/api/jobs/firmware-upgrade/route-preview	Route guard prüfen	preview firmware upgrade routes
POST	/api/jobs/firmware-upgrade/{job_id}/poll-config-deployment	Route guard prüfen	poll firmware upgrade config deployment v11
POST	/api/jobs/firmware-upgrade/{job_id}/refresh-affected-aps	Route guard prüfen	refresh firmware upgrade affected aps
POST	/api/jobs/housekeeping/cancel-stale-queued	Admin	cancel stale queued jobs
POST	/api/jobs/staggered-reboot	Route guard prüfen	create staggered reboot job
GET	/api/jobs/{job_id}	Auth	get job
POST	/api/jobs/{job_id}/cancel	Admin	cancel job

Mobile

Methode	Endpoint	Zugriff	Zweck
GET	/api/mobile/access-points	Route guard prüfen	mobile access points
POST	/api/mobile/access-points/{access_point_id}/client-vlan-tests	Route guard prüfen	mobile access point client vlan test

Methode	Endpoint	Zugriff	Zweck
POST	/api/mobile/access-points/{access_point_id}/dhcp-test	Route guard prüfen	mobile access point dhcp test
POST	/api/mobile/access-points/{access_point_id}/tests/{test_name}	Route guard prüfen	mobile access point test
GET	/api/mobile/clients	Route guard prüfen	mobile clients
POST	/api/mobile/clients/{client_id}/troubleshoot	Route guard prüfen	mobile client troubleshoot
GET	/api/mobile/summary	Route guard prüfen	mobile summary

Monitor / Insight

Methode	Endpoint	Zugriff	Zweck
POST	/api/monitor/collector/collect-now	Admin	Manueller, begrenzter Collector-Lauf
GET	/api/monitor/collector/status	Auth	Collector-Status und effektive Intervalle
POST	/api/monitor/db/initialize	Admin	control monitor db initialize
GET	/api/monitor/db/status	Auth	Monitor-Datenbank- und Storage-Status
GET	/api/monitor/foundation	Auth	get monitor foundation status
GET	/api/monitor/ingestion/status	Auth	control monitor ingestion status
POST	/api/monitor/ingestion/xiq-snapshot/preview	Admin	control monitor xiq snapshot preview
POST	/api/monitor/ingestion/xiq-snapshot/run	Admin	control monitor xiq snapshot run
GET	/api/monitor/live-snapshot/preview	Auth	control monitor live snapshot preview
POST	/api/monitor/live-snapshot/save	Admin	control monitor live snapshot save
POST	/api/monitor/maintenance/confirm-action	Admin	control monitor maintenance confirm action
POST	/api/monitor/maintenance/reset-data	Admin	control monitor maintenance reset data
POST	/api/monitor/maintenance/settings	Admin	Control Settings, Storage oder Logs
GET	/api/monitor/maintenance/status	Auth	control monitor maintenance status
GET	/api/monitor/overview	Route guard prüfen	control monitor overview
GET	/api/monitor/query-contracts	Auth	control monitor query contracts
GET	/api/monitor/read-model	Route guard prüfen	control monitor read model
POST	/api/monitor/scheduler/preview	Admin	control monitor scheduler preview
POST	/api/monitor/scheduler/run-due	Admin	control monitor scheduler run due
GET	/api/monitor/scheduler/status	Auth	control monitor scheduler status
GET	/api/monitor/snapshot-trends	Auth	control monitor snapshot trends
POST	/api/monitor/usage-collect	Admin	control monitor usage collect
GET	/api/monitor/usage-scout	Admin	control monitor usage scout
GET	/api/monitor/workspace	Auth	Scope-basierter Monitor Workspace und Investigation
GET	/api/monitor/xiq-data-source-map	Auth	control monitor xiq data source map
GET	/api/public/monitor/collector/status	Public	Collector-Status und effektive Intervalle
GET	/api/public/monitor/db/status	Public	Monitor-Datenbank- und Storage-Status
GET	/api/public/monitor/foundation	Public	get public monitor foundation status
GET	/api/public/monitor/ingestion/status	Public	control public monitor ingestion status
GET	/api/public/monitor/live-snapshot/status	Public	control public monitor live snapshot status
GET	/api/public/monitor/maintenance/status	Public	control public monitor maintenance status
GET	/api/public/monitor/overview	Public	control public monitor overview
GET	/api/public/monitor/query-contracts	Public	control public monitor query contracts
GET	/api/public/monitor/read-model	Public	control public monitor read model
GET	/api/public/monitor/scheduler/status	Public	control public monitor scheduler status
GET	/api/public/monitor/snapshot-trends	Public	control public monitor snapshot trends
GET	/api/public/monitor/workspace	Public	Scope-basierter Monitor Workspace und Investigation

Methode	Endpoint	Zugriff	Zweck
GET	/api/public/monitor/xiq-data-source-map	Public	control public monitor xiq data source map
GET	/api/public/monitor/xiq-source-catalog	Public	control public monitor xiq source catalog

NAC / Integrations

Methode	Endpoint	Zugriff	Zweck
GET	/api/integrations/servicenow/foundation	Auth	get servicenow foundation status
POST	/api/nac/clearpass/test	Route guard prüfen	test nac clearpass connection
GET	/api/nac/site-engine/summary	Route guard prüfen	get nac site engine summary
POST	/api/nac/site-engine/test	Route guard prüfen	test nac site engine connection
GET	/api/public/integrations/servicenow/foundation	Public	get public servicenow foundation status
GET	/api/public/integrations/servicenow/outbox-preview	Public	control public servicenow outbox preview

Operations / Update / Backup

Methode	Endpoint	Zugriff	Zweck
GET	/api/public/system/env-doctor	Public	control public env doctor
GET	/api/public/system/feature-gates	Public	get public system feature gates
GET	/api/settings	Auth	Control Settings, Storage oder Logs
PUT	/api/settings	Admin	Control Settings, Storage oder Logs
GET	/api/settings/logs/download	Auth	Control Settings, Storage oder Logs
GET	/api/settings/public	Route guard prüfen	Control Settings, Storage oder Logs
GET	/api/settings/storage	Auth	Control Settings, Storage oder Logs
POST	/api/system/backup-schedules/{job_id}/run-now	Auth	run scheduled backup now
GET	/api/system/backups	Auth	Backup / Restore Operations
POST	/api/system/backups/create	Auth	Backup / Restore Operations
DELETE	/api/system/backups/{backup_id}	Auth	Backup / Restore Operations
POST	/api/system/backups/{backup_id}/cancel	Auth	Backup / Restore Operations
PATCH	/api/system/backups/{backup_id}/comment	Auth	Backup / Restore Operations
GET	/api/system/backups/{backup_id}/download	Auth	Backup / Restore Operations
GET	/api/system/env-doctor	Auth	control env doctor
GET	/api/system/feature-gates	Auth	get system feature gates
GET	/api/system/migration-data-dry-run	Auth	get system migration data dry run
POST	/api/system/migration-execute	Admin	post system migration execute
GET	/api/system/migration-execution-dry-run	Admin	get system migration execution dry run
GET	/api/system/migration-full-dry-run-plan	Auth	get system migration full dry run plan
GET	/api/system/migration-postgres-compare	Auth	get system migration postgres compare
GET	/api/system/migration-readiness	Auth	get system migration readiness
GET	/api/system/migration-schema-dry-run	Auth	get system migration schema dry run
GET	/api/system/migration-target-validation	Auth	get system migration target validation
POST	/api/system/monitor-db/check	Auth	check system monitor database
POST	/api/system/monitor-db/initialize	Admin	initialize system monitor database
POST	/api/system/restore/execute	Admin	Backup / Restore Operations
GET	/api/system/restore/maintenance	Admin	Backup / Restore Operations
PUT	/api/system/restore/maintenance	Admin	Backup / Restore Operations
POST	/api/system/restore/prepare-candidate	Admin	Backup / Restore Operations
POST	/api/system/restore/prepare-existing	Admin	Backup / Restore Operations
GET	/api/system/restore/sessions/{restore_session_id}	Admin	Backup / Restore Operations

Methode	Endpoint	Zugriff	Zweck
POST	/api/system/restore/sessions/{restore_session_id}/safety-backup	Admin	Backup / Restore Operations
POST	/api/system/restore/validate-upload	Auth	Backup / Restore Operations
POST	/api/system/setup/complete	Admin	post system setup complete
POST	/api/system/setup/reset	Admin	post system setup reset
GET	/api/system/setup/status	Auth	get system setup status
POST	/api/system/setup/test-nac	Admin	post system setup test nac
POST	/api/system/setup/test-xiq	Admin	post system setup test xiq
POST	/api/system/setup/validate	Admin	post system setup validate
GET	/api/system/status	Auth	get system status
GET	/api/system/update-audit	Auth	Update Planning, Jobs und Execution
POST	/api/system/update-check	Auth	Update Planning, Jobs und Execution
POST	/api/system/update-execute	Admin	Update Planning, Jobs und Execution
GET	/api/system/update-execution/components	Route guard prüfen	Update Planning, Jobs und Execution
POST	/api/system/update-execution/execute	Route guard prüfen	Update Planning, Jobs und Execution
GET	/api/system/update-execution/jobs/{job_id}	Route guard prüfen	Update Planning, Jobs und Execution
GET	/api/system/update-execution/status	Route guard prüfen	Update Planning, Jobs und Execution
GET	/api/system/update-jobs	Auth	Update Planning, Jobs und Execution
POST	/api/system/update-jobs/dry-run	Admin	Update Planning, Jobs und Execution
GET	/api/system/update-jobs/{job_id}	Auth	Update Planning, Jobs und Execution
POST	/api/system/update-plan	Auth	Update Planning, Jobs und Execution
GET	/api/system/update-status	Auth	Update Planning, Jobs und Execution

Reports

Methode	Endpoint	Zugriff	Zweck
GET	/api/public/report-engine/foundation	Public	Report Engine Status, Templates oder Jobs
GET	/api/public/report-engine/jobs/status	Public	Report Engine Status, Templates oder Jobs
GET	/api/public/report-engine/jobs/templates	Public	Report Engine Status, Templates oder Jobs
GET	/api/report-engine/foundation	Auth	Report Engine Status, Templates oder Jobs
GET	/api/report-engine/jobs	Route guard prüfen	Report Engine Status, Templates oder Jobs
POST	/api/report-engine/jobs	Route guard prüfen	Report Engine Status, Templates oder Jobs
POST	/api/report-engine/jobs/preview	Route guard prüfen	Report Engine Status, Templates oder Jobs
GET	/api/report-engine/jobs/status	Route guard prüfen	Report Engine Status, Templates oder Jobs

XIQ / Diagnostics

Methode	Endpoint	Zugriff	Zweck
GET	/api/xiq/access-points	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/access-points/{ap_id}/refresh-now	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/accounts	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/accounts/switch	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/acsp-cli-neighbors	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/cli	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/clients/refresh	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/disconnect-clients	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/management-test	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/packet-capture/start	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose

Methode	Endpoint	Zugriff	Zweck
DELETE	/api/xiq/ap-actions/{device_id}/packet-capture/{job_id}	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/ap-actions/{device_id}/packet-capture/{job_id}	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/packet-capture/{job_id}/archive	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/ap-actions/{device_id}/packet-capture/{job_id}/download	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/packet-capture/{job_id}/stop	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/ping	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/ping-device	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/radio-interfaces	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/reboot	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/traceroute	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/vlan-probe	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/ap-actions/{device_id}/vlan-probe-cli	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/ap-neighbors/{device_id}	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/cache/clear-runtime-and-refresh	Admin	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/cache/refresh	Admin	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/cache/refresh-metadata	Admin	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/cache/status	Auth	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/client-details/{client_id}	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/client-experience/{client_id}	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/client-roaming/{client_id}	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/client-troubleshoot	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/clients/active	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/clients/active/count	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/clients/active/counts	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/clients/live-refresh	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/debug/config	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/devices	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/locations	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/login	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
POST	/api/xiq/nac/scope-test	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/pcap/download-url	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/portal-status	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/token-info	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose
GET	/api/xiq/wlan-config	Route guard prüfen	XIQ-Proxy, Cache oder Diagnose

21.1 Glossar und Quellen

AP: Access Point. Client: Wireless Endpoint. Beam: Remote-Site-Agent. Evidence: Nachweis aus Test, Capture, Log oder Snapshot. Collector: begrenzter Read-only-Erfasser. Snapshot: gespeicherter sanierter Datenstand. Workspace: Scope-basierte Monitor-Antwort. Root Cause: korrelierte Ursache. NAC: Network Access Control. CAPWAP/HiveManager/Telemetry: Management- und Cloud-Kommunikationsdomänen. RPCAP/PCAP: Remote Packet Capture und Paketdatei.

Quellen: backend/main.py Route-Dekoratoren, Monitor-/Report-/Backup-/Update-Module, frontend/src/services/api.js und Monitor-Dokumentation. Der geschützte OpenAPI-Export ist vorhanden, wurde aber ohne Credentials nicht live abgerufen.