

Kernel R1 — Kong and Gateway Operations

Evidence-based handover of the implemented Kernel scope. Business acceptance and release signatures remain open.

UAT package home · Editable UAT and technical registers

1. Kong in the deployed request path

Client HTTPS → Nginx portal virtual host → Kong host route → authenticated HTTPS web/API gateway → module runtime → scoped database function.

Nginx terminates public TLS. Kong maps portal/API host and path to the web/API host. The authenticated host and IAM resolve the current session, domain/profile/roles, permitted menu/screen and control decisions. Axis provides rendering metadata. Successful Kong routing is not an authorization grant and must not bypass native module permissions.

This guide uses the 11 October portal closeout and its pre-change Kong projection plus deployment source. Current live version, plugins and routes have not been re-queried during document preparation. Configuration fields with no retained proof remain confirmation items.

T02 · T22.

2. Routes, service, TLS, policy and management

GW01 · Topology

Item	Value
Recorded implementation	Browser → portal Nginx TLS → Kong proxy 127.0.0.1:8000 → kernel-mediflex HTTPS 127.0.0.1:11440 → authenticated gateway → module runtimes / PostgreSQL.
Source	T02; DP03, DP06–07
UAT/operations confirmation	Confirm active host, routes and upstream before UAT freeze.

GW02 · Recorded Kong version

Item	Value
Recorded implementation	3.9.3 in the pre-portal inspection.
Source	T22
UAT/operations confirmation	Historical version; current installed version not queried by packaging.

GW03 · Public portal route

Item	Value
Recorded implementation	kernel-portal; host portal.kernelhealth.tech; path /; http/https; strip_path=false; preserve_host=true; same existing kernel-mediflex service.
Source	T02; DP06
UAT/operations confirmation	Portal deployment receipt includes created route ID; check current matching route.

GW04 · API compatibility route

Item	Value
Recorded implementation	kernel-mediflex; host api.kernelhealth.tech; path /; strip_path=false; preserve_host=true. Existing API route preserved by portal deployment.
Source	T22; T02; DP03
UAT/operations confirmation	Only recognized UI GET/HEAD entry points redirect to portal; API endpoints retain API behavior.

GW05 · Upstream

Item	Value
Recorded implementation	Service kernel-mediflex; HTTPS 127.0.0.1:11440. Initial provision sets tls_verify=false for the loopback upstream.
Source	T22; DP03
UAT/operations confirmation	Public TLS and upstream TLS are separate. Reconfirm current upstream certificate policy; public certificate verification must stay enabled.

GW06 · Timeouts

Item	Value
Recorded implementation	Initial service settings: connect 10000 ms; read/write 60000 ms.
Source	T22; DP03
UAT/operations confirmation	Runtime and UI deadlines are separate; current values and retry policy require readback. A timeout does not prove a mutation failed.

GW07 · Admin API

Item	Value
Recorded implementation	http://127.0.0.1:8001 in operator configuration.
Source	DP05
UAT/operations confirmation	Keep management local/restricted. Verify listening addresses and NSG/firewall; do not publish an Admin API route.

GW08 · TLS and headers

Item	Value
Recorded implementation	Portal Nginx: TLS 1.2/1.3, HSTS max-age=31536000, route-specific CSP; HTTP redirects to HTTPS except ACME challenge.
Source	DP07; T02
UAT/operations confirmation	Confirm certificate expiry/renewal owner. Never distribute private-key contents.

GW09 · Forwarded request context

Item	Value
Recorded implementation	Nginx preserves Host, X-Real-IP, X-Forwarded-For and X-Forwarded-Proto=https; upgrade headers forwarded.
Source	DP07
UAT/operations confirmation	Verify trusted proxy policy and host/origin validation after any edge change.

GW10 · Authentication ownership

Item	Value
Recorded implementation	Application gateway/IAM handle native session, selected profile and OIDC flow. Portal origin is canonical; registered API-host callback is relayed with state/nonce/PKCE and host-bound flow validation.
Source	T02
UAT/operations confirmation	Kong routing does not replace IAM RBAC/ABAC or independent review.

GW11 · CORS / mutation origin

Item	Value
Recorded implementation	Credentialed trusted-origin handling and mutation-origin rejection are in the authenticated web host. Recorded trusted UI CORS 204 and untrusted origin 403.
Source	T01–02; DP04
UAT/operations confirmation	Do not assume a Kong CORS plugin exists. Reconfirm active allowed origins.

GW12 · Plugins

Item	Value
Recorded implementation	Pre-portal plugin snapshot is empty.
Source	T22
UAT/operations confirmation	No evidence here of enabled Kong JWT/OIDC/rate-limit/WAF/logging plugins; obtain a sanitized current inventory before making those claims.

GW13 · Private service ports

Item	Value
Recorded implementation	Deployment firewall rules restrict application ports, including 9090, 8081, 8080, 10040–10051 and 11440/11442, to loopback ingress.
Source	DP03
UAT/operations confirmation	This is script evidence; current NSG/firewall and Kong exposure need current operations confirmation.

GW14 · Observability

Item	Value
Recorded implementation	Capture HTTP status, correlation_id, timestamp, selected profile, route/upstream and matching systemd/Nginx/Kong logs.
Source	E01; T02; DP03
UAT/operations confirmation	No centralized monitoring/SIEM retention or alerts acceptance is asserted by this package.

3. Read-only baseline collection

From an approved VM administrator session, use local Admin API GETs and whitelist only the required configuration fields. Commands below require jq and local Admin API access; adapt authentication to current management policy. These commands have not been run by this packaging task. Retain outputs in a protected operations record and add a sanitized projection to UAT evidence.

```
kong version
systemctl is-active nginx kong kernel-web.service
curl --fail --silent --show-error http://127.0.0.1:8001/services/kernel-mediflex | jq
'{name,protocol,host,port,connect_timeout,read_timeout,write_timeout,retries,tls_verify}'
curl --fail --silent --show-error http://127.0.0.1:8001/routes/kernel-mediflex | jq
'{name,hosts,paths,protocols,strip_path,preserve_host,service}'
curl --fail --silent --show-error http://127.0.0.1:8001/routes/kernel-portal | jq
'{name,hosts,paths,protocols,strip_path,preserve_host,service}'
curl --fail --silent --show-error 'http://127.0.0.1:8001/plugins?size=1000' | jq '{plugins:
```

```
[.data[]|{name,enabled,service,route,consumer}],next}'  
sudo nginx -t
```

Follow any returned plugin pagination cursor and capture every page. Do not export plugin config, consumer credentials, private keys, session cookies or a raw service environment. Verify actual listen addresses/NSG rules and certificate expiry through authorized operations access. Do not assume the public proxy test proves the management port is private.

4. Verification scenarios and expected interpretation

Scenario	Expected observation	Evidence to retain
Portal HTTP / TLS	HTTP redirects to canonical HTTPS; valid trusted certificate; login loads.	Timestamp, URL/status, certificate validity and redirect target.
API compatibility	API request remains API response; only known UI GET/HEAD bookmarks redirect.	Method/path/status/Location with query secrets redacted.
No authenticated session	Protected API401; protected UI/static routes redirect to sign-in as designed.	Anonymous request; do not count expected401/303 as outage.
Valid session, permitted profile	Native API and permitted dynamic menu/screen load.	Selected assignment/profile, allow decision and application correlation ID.
Valid session, denied permission	403 with native IAM/Axis reason; no data leak or enabled unauthorized action.	Denied resource/control; tenant/domain context.
Untrusted mutation origin	Rejected by web origin policy.	Origin and status; no mutation sent to business owner.
OIDC callback/replay	Bound valid flow completes; invalid state/nonce/PKCE/replay rejected.	Isolated protocol proof and approved interactive sign-in evidence.
Timeout/upstream failure	Preserve correlation and determine whether owner accepted command.	Upstream/readiness, attempt/output ID and owner reconciliation before retry.
Route propagation	New host is matched by Kong before Nginx exposes public virtual host.	DP06 readiness loop; historical3-second delay recorded; do not rely on fixed sleep.

5. Gateway incident triage and recovery

1. Check DNS/TLS and exact host first. If login fails before API routing, inspect Nginx certificate/virtual-host state and Kong proxy readiness.
2. For no matching route, compare host/path/protocol with the active Kong route; preserve_host and strip_path affect application routing and callback validation.
3. For upstream502/503/504, inspect kernel-web readiness, Kong upstream address and bounded service logs. Do not expose internal runtime ports as a workaround.
4. For401, verify session age and host-bound context. For403, verify selected profile/domain and native decision; do not weaken gateway authentication to fix IAM mappings.

5. For 500 DB_EXEC_ERROR, capture correlation_id and use protected runtime/database diagnostics. A visible menu does not establish backend permission or database health.
6. After a failed edge change, follow the exact portal backup/rollback record. Test login, existing API route, callback binding and allow/deny behavior before resuming users.

Support escalation: edge/network → web gateway → IAM/Axis → module/DB owner according to the first failing layer. Retain UTC timestamps and sanitized evidence across layers.

Kernel R1 UAT package • Prepared • Documentation and evidence consolidation only. No application deployment, access grant or business approval was performed by this packaging run.

Current release additions and acceptance

The following changes update the earlier handover baseline. Earlier results retain their original scope. The additional business UAT cases start Not run and require actual tester evidence.

Feature	Module	Change	Operating impact
F01	IAM	Explicit domain/profile mapping	Approved domain creation starts with zero profile links; pending mappings do not grant eligibility.
F02	Axis	Governed screen authoring	Create Screen, source/field definitions, access mapping, draft, preview and originating-record review.
F03	IAM / Axis	Reviews on the owning record	Review pending master, mapping, screen and control changes in their originating workspace.
F04	IAM	Named Super Administrator	Explicit scoped same-person review with administrator evidence; ordinary profiles retain independence checks.
F05	Axis	Screen and control metadata	Screen title/help and control label/help/format maintained through governed presentation changes.
F06	Axis	Owning screen controls	Controls list owning screens first; details and controls share context, refresh and Back behavior.
F07	Pulse / IAM	Notification outcome links	Published notification OPEN contract restored; recipient/context checks retained.
F08	MEDES	Activation qualification	Installed technical package; role grants, enabled APIs and review-route activation remain pending.
F09	Kernel	Documentation hub	Master index, separate manuals/demos/UAT, linked modules, current supplement and offline downloads.

Feature	Module	Change	Operating impact
F10	Axis	Consistent screen authoring and explicit header help	Shared record tabs, responsive form grid, Cancel/Save footer and multiline screen-header help stored in existing metadata.
F11	Axis	Bounded authorized editor options	Prepared authorization context eliminates repeated source checks; source and permission results remain unchanged.

[Feature register](#) · [Additional UAT cases](#) · [New evidence index](#)

MEDES entry gate: technical installation is complete; target activation is incomplete. Role grants, enabled APIs and document-review route must be verified before a live business demo. Provider-based delivery additionally requires approved provider setup and authorized destinations.

Verification boundary: the Axis screen-context release records 35 rollback-only database checks, 12 UI tests and 15 fixture-browser checks. The notification contract correction records 11 schema checks and 17 rollback-only database checks. These are not a complete authenticated production journey or a new client UAT sign-off.