OmniEIR □置参考

□述 | 操作指南 | 指标与监控 | 故障排除

所有 OmniEIR 配置都位于 `:omnieir` 应用程序键下。可以通过环境变量覆盖一部分键，但这仅在 生产运行时□置 (`config/runtime.exs`) 中生效。

□置结构

```
config :omnieir,
  # SBI □听器身份（向 NRF 广播）
  sbi_scheme: "http",
  sbi_addr: "127.0.0.23",
  sbi_port: 7777,

  # NRF 注册
  nrf_uri: "http://127.0.0.10:7777",
  heartbeat_interval: 10_000,

  # 提供的 PLMN（每个部署可覆盖）
  mcc: "999",
  mnc: "70",

  # 包含运营商 EIR 规则的 OmniHSS REST API
  hss_api_base_url: "https://127.0.0.1:8443",

  # OmniHSS API 密钥（角色 eir_lookup）。必填，无默认值。
  hss_api_key: "<OmniHSS API key with role eir_lookup>",

  # 当没有规则匹配所提供设备时返回的判决
  unknown_equipment_status: "WHITELISTED"
```

□□□□

□□	□□	���□	
`sbi_scheme`	□□□	`"http"`	`EIR_SBI_S`
`sbi_addr`	□□□	`"127.0.0.23"`	`EIR_SBI_A`
`sbi_port`	□□	`7777`	`EIR_SBI_P`
`nrf_uri`	□□□	`"http://127.0.0.10:7777"`	`EIR_NRF_U`
`heartbeat_interval`	□□□□□	`10_000`	□
`mcc`	□□□	`"999"`	`EIR_MCC`
`mnc`	□□□	`"70"`	`EIR_MNC`
`hss_api_base_url`	□□□	`"https://127.0.0.1:8443"`	`HSS_API_B`
`hss_api_key`	□□□	□□□□□	□

参数	类型	���认	
`unknown_equipment_status`	字符串	`"WHITELISTED"`	`EIR_UNKNO`

实验室 OmniHSS 的自签名 TLS 证书被接受（`verify_none`），与其他 HSS-REST 消费者（OmniUDR）匹配。在生产环境中，确保 HSS 由受信任的 CA 终止。

OmniHSS 在其 REST API 上使用基于角色的访问控制。没有有效的 `x-omnihss-key` 头的请求会被拒绝，返回 `401`。`hss_api_key` 的值是一个秘密。OmniEIR 不会将其写入日志。在启用 OmniHSS 的访问控制之前，请安装此版本，否则每次读取规则都会失败，EIR 检查将失败并保持开放状态。

规则的□置（**OmniHSS**）

OmniEIR 没有自己的□置 **API**。规则是针对 OmniHSS 创建的，正如 4G S13 接口一样，例如：

```
curl -k -X POST https://<hss>:8443/api/eir/rule \
  -H 'content-type: application/json' \
  -d '{"action":"blacklist","regex":"^35316005"}'
```

- `action` 是 `whitelist`、`blacklist`、`greylist` 之一。
- `regex` 与设备身份字符串进行匹配。规则按 OmniHSS 返回的顺序进行评估；第一个匹配的规则胜出。

AMF 端□置（启用检查）

设备检查由 **AMF** 执行，默认��况下 禁用，因此现有部署不受影响。在 `:omniamf` 键下启用它：

参数	类型	默认	描述
`eir_enabled`	布尔值	`false`	当为 `true` 时，AMF 在注册期间查询 5G-EIR 并拒绝黑名单中的 PEI。
`eir_uri`	字符串 | nil	`nil`	静态 5G-EIR SBI URI。当为 `nil` 时，AMF 通过 NRF 发现 EIR（NFType `5G_EIR`）。

```
config :omniamf,
  eir_enabled: true
  # eir_uri: "http://127.0.0.23:7777"    # 可选；省略以使用 NRF 发现
```

OmniEIR 指标与监控

□述 | 配置参考 | 操作指南 | 故障排除

Prometheus 端点

OmniEIR 通过 `TelemetryMetricsPrometheus` 在 `prometheus_metrics_port`（默认 **9572**）上暴露 Prometheus 抓取端点：

```
GET http://<eir-host>:9572/metrics
```

所有标签都是低基数的（`status` / `result` / `nf_type`），因此系列计数保持有限。

指标

指标	类型	标签	
`omni_eir_equipment_check_count`	counter	`status`	根据解析的 `Equipmen` （`WHITELISTED`/`B` 进行的设备检查计数。
`omni_eir_hss_request_count`	counter	`result`	OmniHSS `GET /` （`success`/`failu`
`omni_eir_hss_request_duration_ms`	gauge	`result`	最近一次 OmniHSS I
`omni_eir_nrf_registration_status`	gauge	`nf_type`	NRF 注册状态（1 = □
`beam_*`	gauge	none	标准 BEAM VM 统计[

基础遥测事件

事件	测量	元数据	由…发出
`[:omnieir, :equipment_check]`	`count`	`status`	OmniEIR 在每个解析的裁决上
`[:omnieir, :hss, :request]`	`count`, `duration_ms`	`endpoint`, `result`	OmniEIR 在每个 `GET /api/eir/rule` 到 OmniHSS 上
`[:omniamf, :eir, :check]`	`count`	`result`（`:whitelisted` | `:greylisted` | `:blacklisted` | `:unknown` | `:error`）	AMF 在每次设备检查时

当黑名单 PEI 阻止注册时，AMF 还会发出其现有的 `[:omniamf, :registration, :result]` 事件，`result: :rejected`。（`[:omniamf, :eir, :check]` 系列在 **AMF** 的 Prometheus 端点上暴露，而不是 OmniEIR 的。）

监控要点

- `[:omnieir, :hss, :request]` 中 `result: :failure` 的上升速率意味着 OmniEIR 无法访问 OmniHSS。AMF 随后会失败开放（每个设备都被允许）。对此进行警报。
- `[:omniamf, :eir, :check]` 中 `result: :blacklisted` 计数被阻止的设备；`:error` 计数 AMF 的失败开放事件。

日志

OmniEIR 和 AMF 记录每个决策。显著的日志行：

- AMF: `5G-EIR 返回 BLACKLISTED 对于 PEI <pei> (<supi>); 阻止注册`

- AMF: `5G-EIR 检查失败对于 <supi> (<reason>); 失败开放`
- OmniEIR: `无法从 HSS 读取 EIR 规则: <reason>`

OmniEIR 操作指南

角色

OmniEIR 是 5G 设备身份注册中心。在用户设备注册期间，AMF 会询问设备的 PEI (IMEI/IMEISV) 是否被允许；OmniEIR 返回 `WHITELISTED`、`BLACKLISTED` 或 `GREYLISTED`。该判决是根据存储在 OmniHSS 中的运营商规则计算得出的。

端点

SBI 监听器暴露了 N5g-eir_EquipmentIdentityCheck 服务 (TS 29.511):

方法	路径	描述
`GET`	`/n5g-eir-eic/v1/equipment-status?pei={pei}&supi={supi}`	返回 `EirResponseData`: `{"status": "<EquipmentStatus>"}`。`pei` 是必需的; `supi` 是可选的。
`GET`	`/n5g-eir-eic/v1/status`	存活探测 (`{"status":"UP"}`)。

`pei` 是 TS 23.003 格式的 PEI: `imei-<15 位数字>` 或 `imeisv-<16 位数字>`。`supi` 是 `imsi-<数字>`。

示例:

```
curl 'http://127.0.0.23:7777/n5g-eir-eic/v1/equipment-status?
pei=imei-353160051234567'
# -> {"status":"WHITELISTED"}
```

消息流

对于 `WHITELISTED` 或 `GREYLISTED` 判决（或任何 EIR 错误），AMF 将继续注册。

匹□逻辑

OmniEIR 反映了 4G S13 决策，因此单个规则集管理两个无线电。给定解析的设备，它会按顺序尝试，并在第一个 `regex` 匹配时停止：

1. 完整的 **IMEISV** 数字字符串（IMEI + 软件版本），然后
2. 单独的 **IMEI**，然后
3. **IMSI**（来自 SUPI）。

如果没有匹配，则返回配置的 `unknown_equipment_status`。

故障开放行为

AMF 端的门控故意设置为 故障开放：如果 EIR 无法访问、返回错误，或者 UE 未提供 PEI，注册将继续。只有明确的 `BLACKLISTED` 判决会阻止设备。这防止了损坏的 EIR 或 HSS 使每个用户都无法使用。需要故障关闭语义的部署在 OmniEIR 上设置 `unknown_equipment_status: "BLACKLISTED"`（因此未匹配的设备被禁止）。请注意，设计上总的 EIR 中断仍然在 AMF 处故障开放。

在部署中启用

1. 在 OmniHSS 中配置规则（`POST /api/eir/rule`）。
2. 启动 OmniEIR；确认它作为 `5G_EIR` 注册到 NRF。
3. 设置 `config :omniamf, eir_enabled: true` 并重启 AMF。
4. 通过手机重启 / UE 重新附加进行验证，并查看 AMF 日志中的 `5G-EIR` 决策行。

OmniEIR 故障排除

□述 | 配置参考 | 操作指南 | 指标与监控

常见问题

尽管我□置了黑名单规则，但每个设备都被允许

请按顺序检查：

1. **AMF** 检查是否启用？默认情况下，门是关闭的。设置 `config :omniamf, eir_enabled: true` 并重启 AMF。没有它，AMF 永远不会查询 OmniEIR。
2. **OmniEIR** 能否访问 **OmniHSS**？读取 `GET /api/eir/rule` 失败 开放（设备 被允许）。在 OmniEIR 日志中注意 `Could not read EIR rules from HSS` 和 `[:omnieir, :hss, :request]` 远程监控，结果为 `result: :failure`。确认 `hss_api_base_url`。确认 `hss_api_key` 已设置并具有 OmniHSS 角色 `eir_lookup`。HSS `401` 表示密钥 缺失或不为 OmniHSS 所知。`403` 表示密钥没有 `eir_lookup` 角色。
3. 正则表达式是否匹□ **UE** 提供的 **PEI**？规则正则表达式是针对 数字字符串进行匹配的。为 14 位 IMEI 编写的��则不会匹配 15 位 `imei-` PEI，除非 正则表达式被锚定以允许它。针对确切的 PEI 数字测试正则表达式。
4. **AMF** 是否实际接收到 **PEI**？如果 UE 没有提供 PEI，AMF 日志 `EIR enabled but UE ... presented no PEI; allowing` 并继续。

AMF 拒绝了我并不打算阻止的设备

- 规则的 `regex` 比预期的更宽泛（例如 `^3531` 匹配整个 TAC 范围）。请缩小范围。
- `unknown_equipment_status` 被设置为 `BLACKLISTED`（失败关闭），且设备不匹配任何规则。要么为其添加一个 `whitelist` 规则，要么恢复为默认的 `WHITELISTED`。

`400 MANDATORY_QUERY_PARAM_INCORRECT`

请求中缺少 `pei` 查询参数 `/n5g-eir-eic/v1/equipment-status`。这是强制性的（TS 29.511）。

来自 **OmniEIR** 的 `500 SYSTEM_FAILURE`

OmniEIR 无法从 OmniHSS 读取规则集。这是上游（HSS）问题；AMF 将非 2xx 视为开放失败。检查 OmniHSS 健康状况和 `hss_api_base_url`。

架构说明

OmniEIR 没有自己的配置 API：IMEI 允许/阻止/灰色规则存储在 OmniHSS 中（与 4G S13 接口共享一个规则集），OmniEIR 通过 HSS REST API 读取它们并应用相同的匹配逻辑。AMF 门设计为开放失败（见 操作），N5g-eir 服务是每个 TS 29.511 的单个 设备状���获取。在 SBI 监听器前的外部代理处终止 TLS。