MOTOTRBO R7 — SCEPman EAP-TLS Enrolment

Overview

How Motorola MOTOTRBO R7 portable radios obtain a device certificate from SCEPman (via SCEP) and authenticate to the WPA3-Enterprise Wi-Fi using EAP-TLS, validated by Aruba ClearPass. SCEPman is Azure-hosted; the radios reach it through an internal Traefik reverse proxy because the R7 SCEP client will not connect to the public Azure endpoint directly.

System	MOTOTRBO R7 / SCEPman / Aruba ClearPass
CA	PBR-ROOT-CA_V1 (SCEPman, Azure App Service)
Radio SCEP hostname	pki-internal.pbr.org.au → Traefik proxy (10.1.8.55)
Main PKI / OCSP hostname	pki.pbr.org.au → Azure direct (untouched by proxy)
Radio VLAN	VLAN 40
Status	Working / verified end-to-end

Why the proxy exists

The R7 SCEP client resolves the SCEP host but will **not open a TCP connection to a public IP** (it connects fine to private/RFC1918 addresses). It also expects a transport it trusts and cannot tolerate the TLS renegotiation Azure App Service triggers under L7 termination. The working solution is a **TCP/TLS passthrough** proxy on a private IP:

- The radio connects to `pki-internal.pbr.org.au` (private IP, the proxy).
- Traefik forwards the raw TLS stream by SNI to the Azure App Service — it does **not** terminate TLS, so there is no Go/Traefik renegotiation failure and no transport-cert substitution. The radio completes TLS end-to-end with Azure's real certificate (which it trusts).
- A separate hostname keeps the radio path isolated: `pki.pbr.org.au` continues to resolve directly to Azure for normal PKI and OCSP, so nothing else is affected.

Azure App Service client-certificate mode stays "Optional Interactive User" (SCEPman's required setting). Passthrough does not have the renegotiation problem that L7 termination did, so this setting does not need changing.

Enrolment runbook (per radio)

Performed in Radio Management. Enrolment is done **at the Kilvington Drive site**, which is the only site that broadcasts the staging SSID. The radio uses the `mototrbo` staging WLAN (WPA2-Personal, password in 1Password) to reach `pki-internal.pbr.org.au` and enrol on boot, then operates on the production `pbrb_radio` WLAN (WPA3-Enterprise, EAP-TLS) which broadcasts at all sites.

Set the following under **General → Wi-Fi Network → Wi-Fi Enterprise Certificates** (both the Common Certificate and Device Certificate entries):

SCEP Server URL	`https://pki-internal.pbr.org.au/static`
CA Identifier	**Optional — leave blank.** Confirmed not required on enrolment (SCEPman is single-CA). May be set to `PBR-ROOT-CA_V1` but is not needed.
Fingerprint (MD5)	`3AF1978B9E4CC55B81C37B372AB2D3BA` (no separators)
Common Name	Per the CN convention below
Challenge Password	From 1Password (SCEPman static challenge) — not stored here
Signature / Key	SHA-256, RSA 2048

Critical: the fingerprint must be the MD5 of the CA cert as returned by the live `GetCACert` response, *not* a copy from a local cert store — they can differ and a mismatch causes the radio to reject the CA ("enrol failed" / "invalid cert"). Derive it with:

```
curl -s "https://pki-internal.pbr.org.au/static?operation=GetCACert" -o ca.bin
openssl x509 -inform DER -in ca.bin -noout -fingerprint -md5
```

After setting the fields, push the codeplug to the radio (confirm the push completes), then enrol over the `mototrbo` staging SSID at Kilvington. Confirm success: a `50`-prefixed issuance appears in SCEPman, and the radio operates on `pbrb_radio` (WPA3-Enterprise).

WLAN / Wi-Fi site scoping

Two WLANs are involved, managed in Aruba Central:

SSID	Security	Purpose	Broadcast scope
`pbrb_radio`	WPA3-Enterprise (EAP-TLS)	Production radio Wi-Fi	**All sites** (no zone)
`mototrbo`	WPA2-Personal (PSK)	Staging / SCEP enrolment only	**Kilvington Drive only** — Aruba Central zone `IT`. Password in 1Password.

Aruba Central zone behaviour: an SSID with no zone broadcasts on all APs in the group; an SSID with a zone broadcasts only on APs that carry the same zone; an AP with no zone broadcasts only the no-zone SSIDs. The `mototrbo` staging SSID is bound to zone `IT`, and only the Kilvington Drive APs carry that zone — so staging is confined to Kilvington while `pbrb_radio` (no zone) remains fleet-wide. *Note: zone `IT` currently means "the Kilvington Drive APs".*

Certificate Common Name (CN) convention

The device certificate CN identifies the radio and, critically, marks it as a **radio device** so ClearPass can authorise it onto the radio VLAN without letting other PBR-CA certificates (DCs, servers, user certs) onto the same network.

Format:

```
<owner-or-role>-<radio-id>.radio.pbr.org.au
```

Example: `IT_Manager-1900.radio.pbr.org.au`

Segment	Example	Meaning
`<owner-or-role>`	`IT_Manager`	The assigned owner or role for the radio.
`<radio-id>`	`1900`	The radio's **Radio ID** (the Radio ID column in Radio Management). Uniquely identifies the radio.
`.radio.pbr.org.au`	`.radio.pbr.org.au`	**The discriminator.** All radio certs carry this suffix; it is what ClearPass matches on to scope access to VLAN 40.

Why it matters: SCEPman issues certificates from the same CA (`PBR-ROOT-CA_V1`) for many device types. "Valid cert from our CA" alone is therefore *not* sufficient to authorise onto the radio network

— a DC or server cert would also pass. ClearPass authorisation matches the `.radio.pbr.org.au` suffix in the CN so that only radios land on VLAN 40.

Rule: every radio device cert CN must end in `.radio.pbr.org.au`. The owner/role and device-id segments should be unique per radio for identification and traceability.

Traefik configuration

Dynamic config on the Docker host (`pbr-docker-kl1`), file provider. Rule file location: `/docker/appdata/traefik3/rules/app-pki.yml`. **TCP passthrough** — Traefik routes on SNI and forwards raw TLS to Azure, never terminating.

```
tcp:
  routers:
    pki-tcp-rtr:
      rule: "HostSNI(`pki-internal.pbr.org.au`)"
      entryPoints:
        - websecure-internal
      tls:
        passthrough: true
      service: pki-tcp-svc
  services:
    pki-tcp-svc:
      loadBalancer:
        servers:
          - address: "app-scepman-cbys7lti43ukq.azurewebsites.net:443"
```

Notes:

- The radio's SNI must match the Azure-bound hostname so App Service routes correctly. The radio sends SNI = the host in its SCEP URL.
- The upstream uses the `azurewebsites.net` name (resolved dynamically) — do **not** hardcode the Azure IP (`13.70.72.33`); it can change.
- The Docker host resolves `app-scepman-cbys7lti43ukq.azurewebsites.net` publicly; `pki-internal.pbr.org.au` resolves (internally) to the proxy — no loop.
- A YAML parse error in the rules file does **not** take the router down — Traefik keeps the last valid config and only logs the error. Always validate the file and check the log for `did not find expected key` after editing.

ClearPass EAP-TLS

EAP-TLS is mutual — both certificates must chain to a CA the other side trusts.

- **Trust the CA:** import `PBR-ROOT-CA_V1` into ClearPass (Administration → Certificates → Trust List), enabled for EAP. This validates the radio device certs.
- **RADIUS / EAP server cert:** must be issued from `PBR-ROOT-CA_V1` (via SCEPman Certificate Master, CSR signed) so the radio trusts ClearPass back. A server cert from any other CA causes the radio to reject the handshake with `unknown_ca`. Generate the CSR on ClearPass, sign in Certificate Master as a **serverAuth** cert, install with the full chain.
- **Authorisation:** match the radio device-cert CN suffix `.radio.pbr.org.au` (see CN convention above) so only radios — not other PBR-CA certs (DCs, servers) — land on the radio VLAN.
- **Enforcement:** radio role → return RADIUS tunnel attributes for **VLAN 40**.
- **OCSP:** revocation checking enforced. ClearPass OCSP override URL points **directly at Azure** (the `pki.pbr.org.au` / `azurewebsites.net` endpoint), bypassing the proxy. Do not route OCSP through the passthrough proxy — passthrough has no HTTP path handling, and ClearPass's OCSP requests would be intercepted and dropped.

Troubleshooting reference

Symptom	Meaning / Fix
Radio resolves SCEP host, no SYN to it (Palo log)	R7 won't connect to a public IP — must use the internal passthrough proxy (private IP).
Connects to private IP but not public	Confirms the public-IP limitation; the proxy is the fix.
"enrol failed" / "invalid cert" after GetCACert succeeds	Fingerprint mismatch. Re-derive MD5 from the live GetCACert response (not a cert store) and re-push.
`tls: no renegotiation` (Traefik upstream)	Caused by L7 termination + Azure client-cert mode "Optional Interactive User". Use TCP passthrough (canonical config) — it avoids the problem entirely.
Traefik 500, `0ms`, `unsupported protocol scheme ""`	Config didn't load — YAML parse error keeps the *previous* config. Check logs for `did not find expected key`; validate YAML; check provider-namespace refs (`@docker` / `@file`).
EAP-TLS `fatal alert by client - unknown_ca`	Radio rejects ClearPass's RADIUS cert. Issue the ClearPass EAP server cert from PBR-ROOT-CA_V1.
EAP-TLS `parse_http_line1 ... OCSP` / no OCSP response	ClearPass OCSP hitting the passthrough proxy (or Azure host-header issue). Point ClearPass OCSP override directly at Azure on `pki.pbr.org.au`.

Symptom	Meaning / Fix
OCSP `Certificate Status revoked, Reason superseded`	Radio is using an old cert that a re-enrolment superseded. Re-enrol cleanly so it holds the current cert. (Also confirms OCSP enforcement works.)

Useful SCEPman log query (Log Analytics) — static SCEP issuances, filtering out OCSP noise:

```
SCEPman_CL
| where TimeGenerated > ago(30d)
| where RequestUrl has "/static"
| order by TimeGenerated desc
```

Maintenance notes

- **Cert renewal:** radios have Renew Strategy = Renew. Verify renewal works through the passthrough path before the first certs expire.
- **Fingerprint:** if the SCEPman Root CA is ever rotated, re-derive the MD5 from GetCACert and update every radio codeplug.
- **CN convention:** every radio device cert CN must end in `.radio.pbr.org.au` or ClearPass will not authorise it onto VLAN 40.
- **Azure IP:** the proxy upstream uses the azurewebsites hostname, so an Azure front-end IP change is handled automatically. Do not pin the IP anywhere.
- **Hostname separation:** keep `pki.pbr.org.au` direct-to-Azure (PKI + OCSP) and `pki-internal.pbr.org.au` → proxy (radio SCEP). Do not point `pki.pbr.org.au` at the proxy — it breaks OCSP.

Revision #6
Created 2026-06-29 04:11:15 UTC by PBR_Documentation
Updated 2026-06-29 04:55:26 UTC by PBR_Documentation