Creating Private Channels

To communicate privately with a group, create a channel with a unique PSK known only to group members. Anyone without the PSK cannot decrypt messages on that channel - **unless** a gateway on that channel uplinks to MQTT without `encryption_enabled`, which republishes the traffic in cleartext to the broker. Channels are encrypted with AES-256-CTR when you use a full 32-byte (256-bit) PSK (a 16-byte key gives AES-128).

Via the App

1. Open the Meshtastic app and go to **Radio Config → Channels**
2. Select an unused channel slot (index 1 - 7; leave index 0 as the public primary unless you have a specific reason to change it)
3. Set a **channel name** (e.g., `TeamAlpha`)
4. Tap **Generate** to create a random PSK, or enter a known PSK manually
5. Save the channel
6. Share the channel URL or QR code with group members out-of-band (signal, in person, etc.)

Via the CLI

Add a new channel (this creates an empty channel at the next free index; do not pass the name to `--ch-add`):

```
meshtastic --ch-add
```

Name the channel and set its PSK on that index. Use `random` to have the firmware generate a strong key, or supply your own base64 key string directly (there is no `base64:` prefix):

```
meshtastic --ch-index 1 --ch-set name TeamAlpha
meshtastic --ch-index 1 --ch-set psk random
```

Export the channel URL for sharing:

```
meshtastic --export-config
```

The config export includes channel URLs that can be shared with other users.

Security Considerations

- **PSK distribution security:** The security of a private channel is entirely dependent on how the PSK is distributed. Share it via an end-to-end encrypted channel (Signal, in person) - not via SMS or unencrypted email.
- **The default LongFast channel is not private.** All Meshtastic users can read it. Never send sensitive information on LongFast.
- **MQTT uplink can leak even a private channel.** If any gateway node on your private channel uplinks to an MQTT broker without `mqtt.encryption_enabled` set, your channel's traffic is republished to the broker in cleartext - so "no PSK = can't read it" only holds for the RF mesh, not for an MQTT-connected mesh.
- **Channel names are not secret.** Only the PSK encrypts message content. The channel name may be visible to other nodes in some circumstances.
- **Changing the PSK:** If a group member's device is lost or compromised, generate a new PSK and redistribute it to all remaining members. The compromised device will no longer be able to decrypt messages after the PSK change. Note there is no per-user revocation and no forward secrecy - rotating the key protects future traffic, but anyone who captured past ciphertext can still decrypt it with the old key.

Position and Telemetry Privacy

By default, position and telemetry are broadcast on channel 0 (the public primary channel). If you want location data to remain within your private group:

1. The simplest, lowest-risk option is to disable position broadcasting entirely: **Radio Config → Position → Position Broadcast Interval → 0**. This keeps you connected to the public mesh while withholding your location.
2. Alternatively, you can make your private channel the primary (index 0). **Be aware of the tradeoff:** putting a private channel at index 0 replaces the default public LongFast primary, which cuts your node off from the public mesh - you will no longer see or be reachable on the public network. Only do this if isolation from the public mesh is intended.

Revision #4
Created 2026-05-03 03:00:27 UTC by Mesh America Admin
Updated 2026-06-09 12:15:09 UTC by Mesh America Admin