

# Sicherheit und Zugriff auf Infrastruktur

Ein öffentlich erreichbarer Repeater ist Infrastruktur und sollte entsprechend administriert werden. Funkreichweite bedeutet, dass ein möglicher Angreifer nicht physisch neben dem Gerät stehen muss, um angebotene Remote-Funktionen zu erreichen.

## Administrationspasswort

Für Repeater und Room Server existieren Passwortfunktionen. Ein produktiver Knoten sollte ein individuelles, nicht triviales Administrationspasswort besitzen.

Reale Passwörter gehören weder in das öffentliche Wiki noch in Screenshots, Git-Repositories oder frei zugängliche Konfigurationsarchive.

## ACL und Berechtigungen

Aktuelle Infrastruktur unterstützt Access-Control- beziehungsweise Permission-Funktionen. Damit können Rechte gezielter vergeben werden, statt Administrationszugang pauschal zu teilen.

## Konfigurationsbackups

Die offizielle Web-Konfiguration kann Einstellungen als JSON exportieren. Solche Backups sind nützlich, können aber sensible Werte enthalten. Sie sollten deshalb nicht automatisch in öffentlich synchronisierte Ordner gelegt werden.

## Physischer Zugriff

Ein Maststandort kann funkseitig gut geschützt und physisch trotzdem leicht manipulierbar sein. Gehäuse, Kabel, Stromversorgung und Befestigung sollten gegen unbeabsichtigtes Öffnen und einfache Manipulation geschützt sein.

## Schlüsselverlust

Vor Änderungen an Identität, Dateisystem oder Firmware muss geklärt werden, welche Schlüssel beziehungsweise Konfigurationen verloren gehen können. Ein unüberlegtes `erase` löscht laut offizieller CLI das lokale Dateisystem und ist kein normaler Neustartbefehl.

## Updates

Sicherheitsrelevante und funktionale Firmwareupdates sollten geplant erfolgen. Vor einem Update sind Versionshinweise, Hardwarekompatibilität und gegebenenfalls Backupmöglichkeiten zu prüfen.

## Öffentliche Dokumentation

Öffentlich sinnvoll sind Knotenname, Funktion, ungefährender Versorgungsbereich und technische Eckdaten. Nicht öffentlich gehören Administratorpasswörter, private Schlüssel, unnötig genaue Zugangsbeschreibungen zu nicht öffentlichen Standorten und sensible Konfigurationsgeheimnisse.

## Quellen, Rechte und redaktionelle Prüfung

- [MeshCore – offizielle Dokumentation](#)
- [meshcore-cli – offizielles Projekt](#)
- [MeshCore Web Config – offizielles Projekt](#)
- [MeshCore Wiki DE – ergänzende Communityquelle](#)

**Redaktioneller Hinweis:** Diese Seite ist eine eigenständige Darstellung für MeshCore Hessen. Sachinformationen wurden anhand der oben genannten Quellen geprüft. Texte, Bilder und die Gliederung des MeshCore Wiki DE wurden nicht übernommen; die Seite wird nur als ergänzende Communityquelle zur Faktenkontrolle genannt. Für technische Details hat die aktuelle offizielle MeshCore-Dokumentation Vorrang. Deutschlandbezogene Funkrechtsangaben werden an den Veröffentlichungen der Bundesnetzagentur geprüft.

**Urheberrecht:** Technische Begriffe, Protokollnamen, Befehlsnamen, Zahlenwerte und andere notwendige Sachangaben werden unverändert verwendet, soweit dies für fachliche Richtigkeit erforderlich ist. Es werden keine längeren fremden Textpassagen oder Bilder reproduziert.

**Prüfstand:** 18. August 2026

---