

# AWS Cloud Infrastruktur Zugänge

**ZUGANGSDATEN** · ZD-2025-007

**Projekt:** AWS Cloud Migration  
**Kunde:** MedTech Solutions AG  
**Datum:** 2025-01-22

## VERTRAULICH

Dieses Dokument enthält vertrauliche Zugangsdaten. Bitte sicher aufbewahren und nicht an Dritte weitergeben.

AWS

Cloud

Produktion

Staging

## AWS Console - Produktion

Amazon Web Services Management Console für Produktionsumgebung

**URL:** <https://medtech-prod.signin.aws.amazon.com/console>

### Technische Einstellungen

**Account ID:** 123456789012  
**Region:** eu-central-1 (Frankfurt)  
**Account Alias:** medtech-prod

### Ports & Protokolle

| Port | Protokoll | Beschreibung  |
|------|-----------|---------------|
| 443  | TCP       | HTTPS Console |

### Zugangsdaten

#### Administrator - IAM Full Access (MFA erforderlich)

**Benutzername:** admin@medtech-solutions.de  
**Passwort:** SSO via Azure AD  
**Typ:** web

#### DevOps - ECS, RDS, CloudWatch, S3

**Benutzername:** devops@medtech-solutions.de  
**Passwort:** SSO via Azure AD  
**Typ:** web

#### ReadOnly - Nur Lesezugriff für Audits

**Benutzername:** readonly@medtech-solutions.de  
**Passwort:** SSO via Azure AD  
**Typ:** web

## Amazon RDS - PostgreSQL

Managed PostgreSQL Datenbank (Multi-AZ)

**URL:** medtech-prod-db.cluster-xxxxx.eu-central-1.rds.amazonaws.com

### Technische Einstellungen

**Engine:** PostgreSQL 15.4  
**Instance:** db.r6g.large (Multi-AZ)  
**Storage:** 500 GB gp3, verschlüsselt (AES-256)  
**Backup:** Täglich, 35 Tage Retention

### Ports & Protokolle

| Port | Protokoll | Beschreibung |
|------|-----------|--------------|
| 5432 | TCP       | PostgreSQL   |

### Zugangsdaten

#### DB Admin - Secret: prod/rds/admin

**Benutzername:** medtech\_admin  
**Passwort:** Gespeichert in AWS Secrets Manager  
**Typ:** database

#### Application User - Secret: prod/rds/app

**Benutzername:** medtech\_app  
**Passwort:** Gespeichert in AWS Secrets Manager  
**Typ:** database

## AWS ECS Cluster

Container-Orchestrierung für Microservices

**URL:** <https://eu-central-1.console.aws.amazon.com/ecs>

### Technische Einstellungen

**Cluster:** medtech-prod-cluster  
**Services:** api-gateway, patient-service, billing-service  
**Task Definition:** Fargate (Serverless)  
**Load Balancer:** ALB (Application Load Balancer)

### Ports & Protokolle

| Port | Protokoll | Beschreibung       |
|------|-----------|--------------------|
| 443  | TCP       | HTTPS (ALB)        |
| 8080 | TCP       | API Gateway intern |

### Zugangsdaten

#### Docker Registry Login via AWS CLI

**Benutzername:** ECR Registry  
**Passwort:** `aws ecr get-login-password`  
**Typ:** api\_key

## GitHub Repository

Source Code und CI/CD Pipelines

**URL:** <https://github.com/medtech-solutions>

## Technische Einstellungen

**Organisation:** medtech-solutions  
**Repositories:** api-gateway, patient-service, infra-terraform  
**CI/CD:** GitHub Actions → AWS CodePipeline

## Zugangsdaten

### Service Account für Deployments

**Benutzername:** medtech-deploy  
**Passwort:** SSH Key oder PAT  
**Typ:** ssh

## Terraform Cloud

Infrastructure as Code State Management

**URL:** <https://app.terraform.io/app/medtech-solutions>

## Technische Einstellungen

**Organisation:** medtech-solutions  
**Workspaces:** prod, staging, dev  
**VCS:** GitHub Integration aktiv

## Zugangsdaten

### Terraform Cloud API Token

**Benutzername:** terraform-cloud  
**Passwort:** Team API Token in 1Password  
**Typ:** api\_key

# Datadog Monitoring

Zentrales Monitoring und Alerting

**URL:** <https://app.datadoghq.eu>

## Technische Einstellungen

**Region:** EU (Frankfurt)  
**Dashboards:** Production Overview, API Metrics, RDS Health  
**Alerts:** PagerDuty Integration aktiv

## Zugangsdaten

### Admin - Vollzugriff auf Dashboards und Alerts

**Benutzername:** devops@medtech-solutions.de  
**Passwort:** SSO via Azure AD  
**Typ:** web

### Sicherheitshinweise

- Bewahren Sie dieses Dokument sicher auf
- Geben Sie Zugangsdaten nicht an Dritte weiter
- Ändern Sie Passwörter regelmäßig
- Verwenden Sie 2-Faktor-Authentifizierung wo möglich
- Melden Sie verdächtige Aktivitäten sofort