COD TACACS+ Module

Network access control (AAA), managed centrally from COD

Who may log in to which switch, and which commands may they run? That is the question TACACS+ answers, yet the server behind it is usually a black box on the command line. The **COD TACACS+ Module** manages your **own in-house TACACS+ server** (authentication, authorization, and accounting per **RFC 8907**) directly from the platform. It works through a hardened backend proxy, fully on-premise and multi-tenant. The frontend never talks to the management API directly.

At a glance: Network AAA per **RFC 8907** • dashboard with health, coverage & role coverage matrix • users, user groups, clients (NAS), and client groups • access control with roles and command sets • **role simulator** against the actual policy • accounting with live log.

Your AAA server, managed from COD

The **Network** → **TACACS+** area controls your own RFC 8907 server through a **hardened backend proxy**, with a dedicated connection per site. The **dashboard** shows health, coverage, activity, and accounting as a customizable widget grid, plus a **role coverage matrix** (user groups × device groups) that makes gaps in coverage visible.

Users, groups, and NAS clients

Manage **users** and **user groups** as well as **clients** (your NAS devices) and **client groups** in one place. Assignments are created via drag and drop. Clients can be managed through their **certificate identity** (IP or DNS mode), DNS clients even without a fixed IP.

Authorization, simulator, and accounting

Under **Access Control** you define authorization rules (PERMIT/DENY), **roles**, and pattern-based **command sets**. The **role simulator** evaluates *user* × *client* × *command* against the actual policy, without contacting anything real. **Accounting** records every session, with filters, detail rows, and an optional **live log**.

Know who may do what, and where. See COD live in your environment, with no sales pressure.

extoco.de • extocode GmbH