# Module 16 – Operator Role Mapping & Admin Twin Lockdown

Module ID: OPS-LOCK-016

Version: 4.1 (Revised CTO Edition)

Layer: Operational Stack & Sovereign Control

Status: RELEASE

Dependencies: Module 00, Module 03, Module 15

## 0. Purpose & Enforcement Point

This module defines the role assignment, privilege enforcement, and admin twin control logic for sovereign operations in MaxOneOpen v4.1. It guarantees that all administrative powers are scope-limited, session-verified, and cryptographically bound to identity capsules. No implicit privilege elevation or orphaned admin control is permitted.

## 1. Role Mapping Schema, Scope Graph & Invocation Rules

All operator roles are declared using a `Role Mapping Capsule (RMC)`:  
`{ role\_id, actor\_id, scope\_map, trust\_tier, expiration, escalation\_flags, timestamp }`  
Scope Map defines domain boundaries, control zones and override limits.  
Invocation: `ASSIGN\_ROLE(actor\_id, role\_id, scope\_map)` (only via certified Admin Twin)

## 2. Admin Twin Structure, Lockdown Protocol & Session Anchoring

The Admin Twin is a cryptographically enforced control construct which:  
- validates scope and session integrity for any role-related call  
- logs all access via `Admin Session Capsule (ASC)`  
- triggers lockdown (`ADMIN\_LOCKDOWN()`) upon trust breach, unauthorized override or forensic event flag  
- enforces rollback of privileges via `LOCKDOWN\_REVOKE()` capsule

## 3. Operator Session Monitoring & Privilege Scope Enforcement

All operator sessions are monitored for:  
- scope compliance  
- unauthorized escalation  
- trust tier drop or misalignment  
- non-conform audit trail  
Detected violations result in:  
- session termination  
- privilege rollback  
- Admin Twin lockdown state trigger

## 4. Capsules, Escalation Events & Forensic Review Anchors

Operational security capsules include:  
- `Role Mapping Capsule (RMC)`  
- `Admin Session Capsule (ASC)`  
- `Privilege Violation Capsule (PVC)`  
- `Lockdown Revoke Capsule (LRC)`  
All are stored in LedgerSync (Module 13) and reviewed via forensic queries (Module 14).

## 5. Intermodular Enforcement Links

This module links to:  
- Module 01 (Execution Control) for role-bound invocation gating  
- Module 03 (Identity) for actor-role coupling  
- Module 05 (ConfigBinding) for rule-linked enforcement  
- Module 12 (Trust) for tier validation  
- Module 13 (LedgerSync) for privilege change trace  
- Module 14 (Audit) for violation path reconstruction

## CTO Validation Matrix

Module 16 (CTO Edition) guarantees the following verifiable conditions:  
- All roles are scope-mapped, trust-linked and declared via capsules: YES  
- Admin control is session-bound, lockdown-capable and traceable: YES  
- Unauthorized privilege changes trigger lockdown and rollback: YES  
- Forensic roles can reconstruct all session and escalation chains: YES  
- No privilege is orphaned, untraced, or beyond capsule control: YES