# Module 05 – ConfigBinding: Runtime Rule Injection & Enforcement Engine

Module ID: CORE-BIND-005

Version: 4.1 (Revised CTO Edition)

Layer: Core Architecture Layer

Status: RELEASE

Dependencies: Module 00, Module 01, Module 04

## 0. Purpose & Enforcement Point

This module defines the real-time rule enforcement engine for MaxOneOpen v4.1. It ensures that every runtime execution is bound to manifest-declared rules, identity-scope constraints, and trust policy filters. All enforcement decisions are logged, conflict-resolved, and auditable as runtime capsule events.

## 1. Binding Logic, Injection Flow & Invocation Schema

ConfigBinding dynamically injects governance rules into the execution flow via the following process:  
1. Retrieve manifest-linked rules from Module 04 (MaxReg)  
2. Evaluate trust, scope, and role compliance  
3. Inject approved rules into the runtime capsule  
4. Enforce evaluation outcome and commit trace  
Invocation schema:  
`BIND\_EXEC\_RULES(manifest\_id, identity\_token, operation\_type)` → returns `BIND\_RESULT` or `BIND\_VIOLATION\_Capsule`

## 2. Conflict Resolution, Rule Priority & Evaluation Outcomes

If multiple rules apply, ConfigBinding evaluates them in defined order:  
- SYSTEM > ROLE > TRUST > AI > AUDIT  
Evaluation outcomes:  
- ALLOW: operation proceeds  
- BLOCK: operation stopped with capsule reason  
- ESCALATE: only allowed via Escalation Capsule (Module 16)  
Each evaluation path is logged as a `Runtime Binding Capsule (RBC)` and linked to the originating manifest and rule IDs.

## 3. Injection Capsule Schema & Runtime Artifacts

Each runtime rule injection creates the following capsules:  
- `Runtime Binding Capsule (RBC)` – includes bound rule set, hash anchors, and enforcement result  
- `Rule Conflict Capsule (RCC)` – if incompatible or unresolved rule set encountered  
- `Binding Trace Snapshot (BTS)` – overview of the decision graph at runtime  
RBC Schema:  
`{ capsule\_id, exec\_session\_id, rule\_ids[], manifest\_id, result, anchor\_hash, timestamp }`

## 4. Intermodular Bindings & Enforcement Hooks

ConfigBinding operates as a central runtime gateway for rule execution and connects with:  
- Module 01 (Execution Control) for enforcement entry point  
- Module 04 (MaxReg) for rule source  
- Module 12 (Trust Enforcement) for trust-tier filtering  
- Module 14 (Audit) for trace logging  
- Module 16 (Admin Twin) for override authorization

## CTO Validation Matrix

Module 05 (CTO Edition) guarantees the following verifiable conditions:  
- All runtime executions receive rule injection from manifest-bound sources: YES  
- Conflicts are resolved in priority order and logged: YES  
- Escalation requires admin capsule logic: YES  
- Audit logs capture rule decisions, scope context, and runtime conditions: YES  
- No runtime operation bypasses rule binding or trust checks: YES