# MaxSuite – Temporary Overrides and UI Isolation

Version: 1.0

Module ID: CTO-T2

Document Type: Emergency Access and Runtime Control

---

## 1. Purpose

This document defines the conditions under which temporary overrides can be applied to MaxSuite AppCapsules, and how the user interface layer is isolated from policy-critical execution paths.

## 2. Allowable Temporary Overrides

Temporary overrides are allowed only if explicitly declared in the associated policy capsule.  
Allowed fields:  
- `override\_id`  
- `valid\_from`, `valid\_until`  
- `signed\_by`  
- `reason\_code` (e.g. EmergencyUpdate, LegalIntervention)  
  
Overrides must:  
- Be signed with a registered authority  
- Be time-limited and auditable  
- Trigger override=true in audit log schema

## 3. Restrictions and Limitations

- Overrides cannot disable capsule boundary checks.  
- Overrides must not unlock unrestricted file, screen, or network access.  
- Overrides expire automatically upon policy update or runtime timer.

## 4. User Interface Isolation

All UI components must:  
- Run within isolated UI sandboxes (e.g. secure WebView, AppFrame)  
- Be prohibited from triggering policy actions directly (no unmediated file exports, camera access etc.)  
- Only act on signals provided by the role-verified runtime shell

## 5. Audit and Escalation

Each override usage must be recorded via MaxAudit and cross-linked to runtime and user role. All override attempts must be traceable to a signer and time window.  
Unrecognized overrides must freeze execution and trigger escalation.