

SMARTCYCLE

Security Management System



The SmartCycle Security Management System is a four-part system designed to work as one. It contains the following:

SmartCycle C4

SmartCycle Lock

SmartCycle Mobile App

The Admin Console

The SmartCycle C4

The SmartCycle C4 is a power source for the locking mechanism in our products. It powers and controls the access system. It is one of the core operations technologies that enables the SmartCycle access ecosystem. Although the physical enclosures may vary, all devices operate on the same standardized SmartCycle lock platform, which is a unified system

that integrates mechanical components, embedded electronics, and secure software architecture. It is designed to function reliably in any environment and guarantees safe operational workflow and efficiency in handling our products. **It provides cross-team compatibility (electrical, bridge maintenance, roadway crews and contractors).**

The lock remains inactive until the C4 is physically attached. This ensures:

- No standby power draw
- No battery replacement cycles (maintenance free design)
- No remote attack surface while idle

Key Features

- Designed to be compatible with the entire SmartCycle product ecosystem, enabling consistent access across multiple product types. Standardized access across teams means little to no training required.
- App Based multi factor authentication to prevent unauthorized access.
- The C4 brings power only when access is needed
- No fixed wiring, no standby power, no battery replacement
- Power is supplied during each authorized visit by design
- The C4 exists specifically to avoid maintenance and permanent power altogether.

Security Management System

SmartCycle Lock (Embedded System)

Each secured unit contains a SmartCycle electronic module designed to operate as the core embedded intelligence of the locking system. This module activates only when powered by the C4 hardware key, ensuring that the lock remains electronically dormant unless intentional access is being attempted. Once powered, it receives encrypted Bluetooth communications, performs authentication validation, and executes secure lock/unlock commands based on

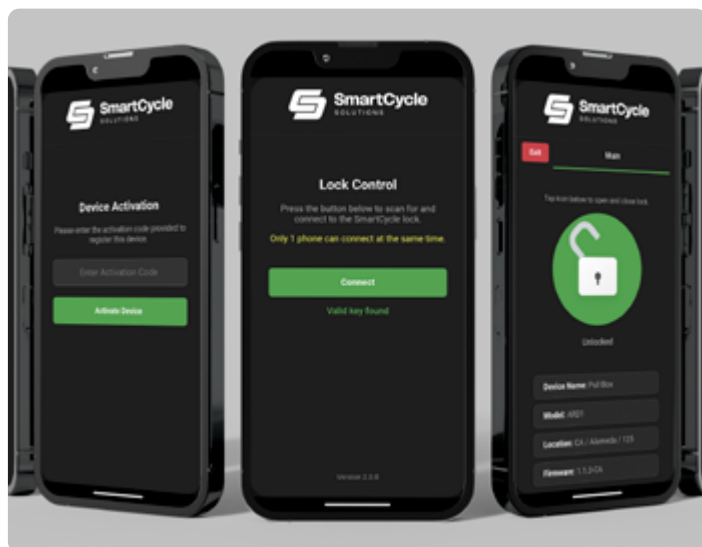
verified credentials. In addition to access control, the module logs every access event to create a reliable activity history. The same embedded architecture is installed across electrical junction boxes, soffits, doors, and other secured enclosures, creating a standardized and unified locking framework across all device types. This uniformity simplifies deployment, strengthens security consistency, and ensures predictable performance in every application.



SmartCycle Mobile Application (Bluetooth Interface)

The SmartCycle mobile application functions as the secure communication bridge between authorized personnel and the embedded lock hardware. Installed exclusively on approved smartphones, the application communicates with powered locks using encrypted Bluetooth Low Energy (BLE) technology. It securely stores time-restricted digital keys that are issued through the cloud management system and are engineered to operate reliably even in offline field environments where cellular service may be unavailable. When connectivity is restored, the app synchronizes permissions, access updates, and event logs with the cloud to maintain system integrity.

Importantly, the application does not independently grant access. It must first detect a lock that has been powered by the C4 device, present a valid digital key, and complete encrypted authentication with the embedded module. In this model, the smartphone serves strictly as a secure digital credential carrier rather than a standalone access authority.

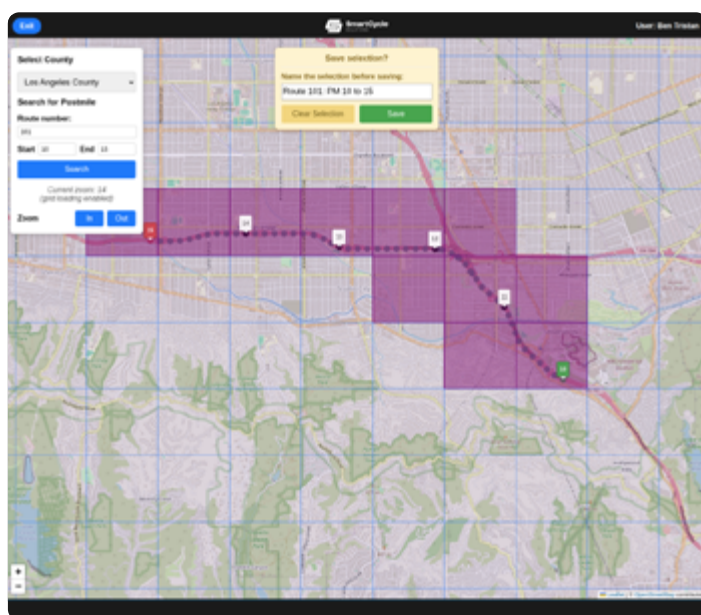
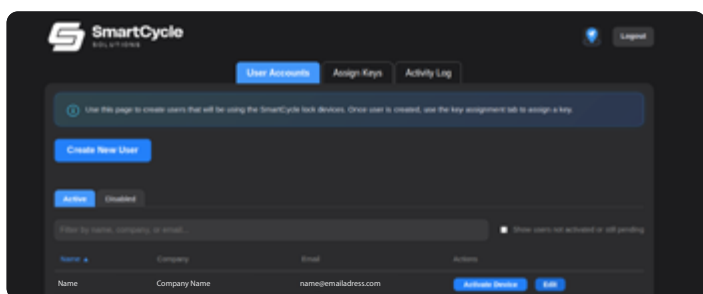
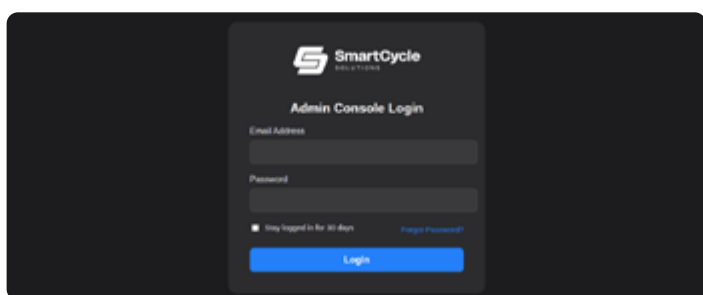


Security Management System

Cloud-Based Management System (Administrative Console)

The cloud-based management platform serves as the central administrative authority and decision-making engine for the entire SmartCycle ecosystem. It governs smartphone authorization within the system and controls the issuance of virtual digital keys. Administrators can define granular permissions based on time windows, geographic considerations, user roles, and specific device types. The platform allows immediate revocation of access rights when necessary, ensuring rapid response to

personnel changes or security concerns. In addition, it maintains comprehensive audit trails of all system activity and preserves a real-time inventory of every deployed device. The cloud ultimately determines which phones are permitted access, which specific units they may interact with, and under what defined conditions. Digital credentials originate in the cloud and are securely synchronized to authorized mobile devices, maintaining centralized control while enabling distributed field access.



Multi-Layer Authentication Model

The SmartCycle system is built upon a multi-layer authentication structure that requires three distinct components for access approval.

- 1 The physical C4 hardware key must be present to power the embedded lock module.
- 2 An authorized smartphone must be used as the credential carrier.
- 3 A valid cloud-issued digital key must be presented and successfully authenticated.

This layered approach ensures that no single compromised element can independently grant entry. **Possession of a lost or stolen C4 device alone cannot unlock equipment. Likewise, a compromised login or digital credential without physical presence cannot activate a lock.** By requiring both physical hardware and digitally validated authorization, the system establishes a dual-dependency security model that significantly exceeds the protection level of traditional mechanical or single-factor electronic lock systems.



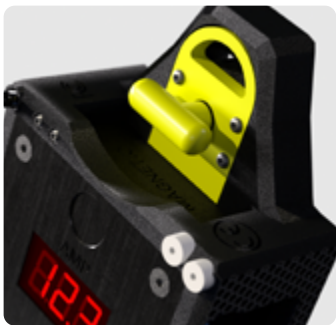
Security Management System

Technical Specifications

PARAMETER	SPECIFICATION
DEVICE TYPE	Proprietary electronic access controller / lock
AUTHENTICATION	App-based multi-factor authentication (2–3 steps)
ACCESS METHOD	Bluetooth-enabled secure authorized access
POWER SUPPLY	Proprietary Power source
INTEGRATION	Designed for SmartCycle secured products (pull boxes, junction lock systems, doors)
SECURITY ARCHITECTURE	Tamper-resistant access mechanism (prevents defeat with common tools)
OPERATING ENVIRONMENT	Roadside / freeway-grade durability for harsh conditions
STANDARDIZATION	Supports role-based access protocols & operational integrity

Advantages

- Prevents unauthorized entry into critical electrical and lighting infrastructure
- Reduces wire theft and vandalism incidents across high-risk zones
- Supports accountability and controlled access for crews and contractors via authentication workflow
- Improves maintenance efficiency through fast secure access
- Enhances overall roadway safety by reducing repeat damage and infrastructure downtime
- Enables to scale a consistent security standard across multiple asset types



Ordering Information

- Model:** SmartCycle C4 Device — Access Controller & Opening Mechanism
- Options:** Standard or custom integration for SmartCycle products; configuration based on asset type
- Lead Time:** 6–8 weeks typical production

Contact: +1 (415) 935-6477
sales@smartcyclesolutions.com | smartcyclesolutions.com

