

Smart Lock Management System Solution

Newcapec Electronics Co., Ltd.

September 2026

Table of Contents

I. Industry Background	1
1.1. Background	1
1.2. Pain Points of Traditional Models	1
II. Product Overview	2
2.1. Product Positioning	2
2.2. Design Concept	2
III. Deployment Diagram	错误！未定义书签。
IV. Core Functions	3
4.1. Function Matrix	3
4.2. Access Permission Management	4
4.3. Personnel Management	7
4.4. Device Management	8
4.5. Mobile App Functions (Optional)	8
4.6. System Management	9
V. Supporting Hardware Terminals	10
5.1. Smart Lock Devices	10
VI. Application Scenarios	11
6.1. Office Scenario	11
6.2. Dormitory / Residence Hall Scenario	11
6.3. Classroom / Laboratory Scenario	错误！未定义书签。
VII. Server Requirements	12
7.1. Operating System	12
7.2. Configuration Requirements	12
7.2.1. Option 1: Separate Application and Database Servers	12
7.2.2. Option 2: Integrated Deployment of Application and Database	12
VIII. Network Requirements	12

一、 Industry Background

1.1. Background

As smart campuses and smart industrial parks accelerate development, access management, as the first line of defense in the security system, is undergoing a profound shift from "fragmented control" to "integrated intelligent management." In traditional deployments, smart locks managed by different areas and departments operate independently, with fragmented permissions, data silos, and cumbersome O&M, making it difficult to meet the modern campus and enterprise requirements for security, convenience, and intelligence.

1.2. Pain Points of Traditional Models

- ❖ **Dispersed Devices and Fragmented Management:** Smart locks deployed independently by different areas and departments door locks are supplied by different vendors and managed on separate platforms. Permissions must be configured repeatedly, data cannot be shared, and O&M costs remain high.
- ❖ **Limited Authentication Methods and Poor User Experience:** Reliance on physical cards or keys means users cannot enter if they forget them. Visitor and temporary-personnel processes are cumbersome, with insufficient convenient identity-authentication options.
- ❖ **Data Silos and Limited Insight:** Access data is scattered across subsystems and cannot form a unified view. Security warnings for abnormal behavior, dormitory return analysis, and similar scenarios lack data support, leaving management in a "passive response" mode.

二、 Product Overview

2.1. Product Positioning

The Smart Lock Management System is an intelligent smart-lock management platform for campuses, enterprises, and industrial parks. Based on the design principles of "one platform, all device types, unified authentication," it brings smart locks across multiple areas onto a unified management platform, creating a closed-loop lifecycle covering device deployment, permission assignment, access control, and data analysis.

2.2. Design Concept

- ❖ One Person, One Profile: Create a unified identity profile for each person, enabling one person, one credential, one authorization, and access across all scenarios while avoiding duplicate entry and fragmented permissions across multiple systems.
- ❖ Multi-Credential Authentication: Supports multiple authentication methods, including cards, QR codes, and facial recognition, enabling users to access smart-lock scenarios seamlessly with the same identity credential.
- ❖ Centralized Device Management: A single platform integrates management processes for all types of access devices and covers the entire lifecycle from deployment and O&M to monitoring, greatly simplifying operations.

三、 Application Overview



四、 Core Functions

4.1. Function Matrix

Function Module	Core Capabilities
Access Permission Management	Operations dashboard, authorization management, authorized-access query, identity-based authorization policies, door-opening passwords, and access data details
Personnel Management	Personnel information maintenance, hierarchical authorization, and organizational structure management
Device Management	Device information, area information, device parameter management, device groups, real-time device monitoring, and OTA remote upgrades
Mobile App Functions (Optional)	Door Opening Assistant (administrator remote opening / user virtual card)
System Management	System parameter configuration, role and permission management, and operation audit logs

4.2. Access Permission Management

Access Permission Management is the core business hub of the system, providing end-to-end management from the data dashboard to access control:

- Operations Dashboard:** Displays key indicators in real time, including device-category summaries, connection status, access details, entry/exit rankings, and alert data.



- Authorization Management:** Supports batch or individual authorization and flexible access-permission configuration by area, time period, and device group.

名单类型: **切换** 设备通用名单

按部门 按人员 按人员标签

说明: 按部门树定位到具体班级等叶子节点, 仅叶子节点可作为查询条件, 单击后触发右侧查询。

Q 按部门名称搜索

- 新开普大学
 - 历史学院
 - 国际学院
 - 安全学院
 - 出入应用事业部**
 - 新开普大学校友会

授权的人员信息 当前查询维度: 按人员 (出入应用事业部)

设备 区域

以下仅展示组长设备的授权配置; 与该组长同组的组员设备同样享有上述授权。

人员信息: 请输入姓名/人 设备名称/序列号: 请输入

搜索 重置

添加授权 复制授权 取消授权 清空授权

当前表格已选择 0 项 清空

☐	设备名称	设备组	设备序列号	区域全称	姓名	人员编号	有效期	创建时间	操作
☐	203房间-正式		4931525062010119	2号楼/...	张...	210805	长期授权	2026-...	取消授权 编辑时间
☐	203房间-正式		4931525062010119	2号楼/...	吴...	130503	长期授权	2026-...	取消授权 编辑时间

共 2 条 10条/页 < 1 > 前往 1 页

- **Authorized Access:** Visually displays relationships among authorized personnel, devices, and areas, with support for quick search and adjustment.

人员信息: 请输入姓名/人员编号 区域/设备: 请选择区域/设备 下发状态: 全部 授权状态: 有效

名单类型: 设备通用名单 所在部门: 请选择部门 设备序列号: 请输入设备序列号

搜索 重置

导出

☐	区域/设备	姓名	人员编号	所在部门	区域全称	设备序列号	介质列表	授	操作
☐	203房间-正式	王...	171130	新开普大学-出入应用事业部	2号楼/2层/203房间	4931525062...	卡 密码		授权关系
☐	203房间-正式	林...	20252161	新开普大学-安全学院-信...	2号楼/2层/203房间	4931525062...			授权关系
☐	203房间-正式	吴...	130503	新开普大学-出入应用事业部	2号楼/2层/203房间	4931525062...	卡 密码 ...		授权关系
☐	203房间-正式	张...	210805	新开普大学-出入应用事业部	2号楼/2层/203房间	4931525062...	卡 密码		授权关系
☐	人脸平板1	张...	9000000...		武汉大学/梅园1舍	333			授权关系

共 5 条 10条/页 < 1 > 前往 1 页

- **Identity-Based Authorization Policies:** Supports differentiated authorization policies based on identity type, organizational structure, time period, and other dimensions.

新增授权规则

* 名单类型

设备通用名单

* 设备范围

请选择设备维度及范围

选择设备

已选维度: 未选择

* 人员范围

请选择人员维度及范围

选择人员

已选维度: 未选择

* 有效期

☒ 长期授权
 ☐ 短期有效

备注说明

最多100个字符

0/100

重置

保存

- Door-Opening Password:** Configures an independent door-opening password for each person as an additional authentication method alongside cards and facial recognition.

编辑

设置门锁初始密码:

用户可使用初始密码开门, 请尽快至移动端修改个人开门密码

☒ 不设初始密码: 用户可在移动端自行设置个人开门密码
 ☐ 身份证后6位
 ☐ 手机号后4位+2位自定义数字

- Access Data:** Records complete details for every access event and supports multidimensional query and export by person, location, and time period.

区域 部门 设备

- ▶ 1号楼
- ▶ 2号楼
- ▶ 武汉大学
- ▶ 测试密钥下发
- ▶ 网关区域
- ▶ 行知园2

起止日期: 2026-06-24 00:00:0 - 2026-06-30 23:59:5

姓名:

人员编号:

认证方式:

人员类型:

身份:

导出

搜索

重置

☐	#	通行时间	姓名	人员编号	人员部门	人员身份	操作
☐	1	2026-06-24 18:20:0 5	测试人员.	20260600011	出入应用事业部	在职人员	
☐	2	2026-06-24 18:20:0 5	测试人员.	20260600011	出入应用事业部	在职人员	
☐	3	2026-06-24 10:52:3 9	测试人员.	20260600011	出入应用事业部	在职人员	
☐	4	2026-06-24 10:52:3 1	测试人员.	20260600011	出入应用事业部	在职人员	
☐	5	2026-06-24 10:24:5 4	测试人员.	20260600011	出入应用事业部	在职人员	

共 9 条

10条/页

<

1

>

前往 1 页

4.3. Personnel Management

Creates unified personnel identity profiles and supports tree-based organizational management, hierarchical role-based authorization, and facial-data enrollment and management. Personnel information is linked with the one-card foundation platform, so processes such as new-student onboarding, dormitory transfers, and departures automatically trigger permission changes, achieving "enter once, apply across all scenarios."

4.4. Device Management

Provides centralized management for all types of smart locks, including device registration, parameter configuration, grouping, real-time status monitoring, and OTA remote upgrades.

4.5. Mobile App Functions (Optional)

Provides mobile applications for both administrators and end users. The administrator app supports remote door opening, one-click inspection, and real-time alert viewing; the user app supports mobile virtual-card access, QR-code scanning in either direction, and dormitory entry/exit queries.



4.6. System Management

Provides system parameter configuration, hierarchical role and permission management, operation audit logs, and other management capabilities to ensure system operations are traceable, auditable, and controllable.

角色名称:
角色别名:

☐	#	角色名称	角色别名	角色排序	操作
☐	1	管理员	admin	2	查看 编辑 删除 更多 ▾
☐	2	访客	visitor	3	查看 编辑 删除 更多 ▾
☐	3	用户	user	4	查看 编辑 删除 更多 ▾
☐	4	家属	family	5	查看 编辑 删除 更多 ▾
☐	5	参数审批员	paramApproval	9	查看 编辑 删除 更多 ▾
☐	6	业务管理员	Business	10	查看 编辑 删除 更多 ▾
☐	7	业务管理	Busi	11	查看 编辑 删除 更多 ▾
☐	8	在职人员	work	12	查看 编辑 删除 更多 ▾

[用户管理](#)
[运营看板](#)
[设备监控](#)
[用户人脸管理](#)
[授权流程](#)
[审计日志](#)

模块名:
操作类型:

①选择模块名称, 操作类型 ②点击搜索查询

☐	#	记录编号	操作人	所在部门	操作时间	模块名	操作类型	描述信息	操作
☐	6	2887432800460	admin	新开普	2023-05-11 13:03:54	内容信息管理	修改	修改内容联动配置	
☐	7	2887431859148	admin	新开普	2023-05-11 13:03:51	内容信息管理	修改	修改内容联动配置	
☐	8	2887427319244	admin	新开普	2023-05-11 13:03:33	内容管理	修改	新增	
☐	9	2887416976588	admin	新开普	2023-05-11 13:02:53	移动端岗位权限管理	修改	新增或修改移动端岗位 权限, 岗位: 288726480 9676授权菜单: 1授权 开门介质: 1,2,3,4	
☐	10	2887414858956	admin	新开普	2023-05-11 13:02:44	移动端岗位权限管理	修改	新增或修改移动端岗位 权限, 岗位: 288726064 0460授权菜单: 1,2,3授 权开门介质:	

共 26 条
10条/页
1 2 3
前往 1 页

五、 Supporting Hardware Terminals

5.1. Smart Lock Devices

Product Category	Representative Model	Core Capabilities
Wireless Networked Smart Lock	I318 Series / I316 Series	Supports multiple communication methods including 4G/Wi-Fi/LoRa/SUB-1G, chip-level encryption, low-battery warnings, tamper alarms, and remote permission issuance
Intelligent Data Collector	SUB-1G Base Station / LoRa Base Station	Wireless collection and forwarding of smart-lock data, support for large-scale

		smart-lock networking, and stable low-power transmission
--	--	--

六、 Application Scenarios

6.1. Office Scenario

- **Unified Authorization and Hierarchical Management:** By campus, building, and floor, sub-administrators can be assigned to authorize and maintain access permissions for personnel in their departments.
- **Administrative Management with Intelligent Linkage:** Door-opening records can serve as attendance records; integration with smart-building systems enables whole-office automation.
- **Flexible Control for Secure and Convenient Access:** Supports normally open mode, scheduled locking, temporary passwords, remote door opening, and automatic alert reporting.
- **Space Asset Optimization and Improved Efficiency:** Big-data analysis identifies underused offices and provides a basis for space-asset management decisions.

6.2. Dormitory / Residence Hall Scenario

- **Linked Permissions with No Manual Configuration:** For new residents, room transfers, and departures, door-opening permissions are linked to accommodation assignments with one click.
- **Efficient Dormitory Management:** One-click door opening, one-click inspection, and remote door opening reduce manual workload.
- **Multiple Security Measures:** Door-close reminders, dynamic temporary

passwords, tamper alarms, chip-level encryption, and other security strategies.

- **Data-Supported Accommodation Decisions:** Provides accommodation analytics including dormitory return analysis, door-opening time analysis, late returns, and multi-day absences.

七、 Server Requirements

7.1. Operating System

All servers use the Ubuntu operating system.

7.2. Configuration Requirements

7.2.1.Option 1: Separate Application and Database Servers

Supported Scale: **Up to 2,000 smart locks**

Application Server × 1: 8 cores / 16 GB RAM

Database Server × 1: 8 cores / 16 GB RAM

7.2.2.Option 2: Integrated Deployment of Application and Database

Supported Scale: **Up to 1000 smart locks**

Server × 1 (integrated application and database deployment): 8 cores 16G, storage 500GB

八、 Network Requirements

System deployment requires network connectivity between two types of nodes: client computers and the application server:

- **Client Computer:** Must be able to access the Internet (to download IoT platform applications) and the application server (to receive/push the installation

package). If Internet access is unavailable, prepare an offline installation package in advance.

● Application Server:

Ports Required for Platform Access			
Port	Required	Purpose	Access Target
9080	Required	Container platform access port	Client computer used for administration and O&M
9085	Required		Client computer used for administration and O&M
30100	Required	Access management system administrator portal access port	Used for administration and O&M by the client computer
30180	Required		Used for administration, O&M, and daily operation by the client computer
22080	Required	Management page access port for the integrated IoT scheduling service	Client computer used for administration and O&M
31306	Optional	Access port for the integrated MySQL database	Client computer used for administration and O&M

● Ports Required by Terminal Devices:

Ports required by smart lock devices			
Port	Required	Purpose	Access Target
28972	Optional	Lora Smart Lock gateway	gateway Device
21883	Optional	4G/Wi-Fi Smart Lock	Smart Lock Device
22035	Optional	Base station for SUB-1G smart locks	Base Station Device
28081	Optional	For smart locks not commissioned through the simplified process, the mobile phone must access this port when commissioning devices via NFC.	The mobile phone can connect to this port over Wi-Fi.